

Group extensions over infinite words*

Volker Diekert

Alexei Myasnikov

February 8, 2011

Abstract

We construct an extension $E(A, G)$ of a given group G by infinite non-Archimedean words over an discretely ordered abelian group like \mathbb{Z}^n . This yields an effective and uniform method to study various groups that "behave like G ". We show that the Word Problem for f.g. subgroups in the extension is decidable if and only if and only if the Cyclic Membership Problem in G is decidable. The present paper embeds the partial monoid of infinite words as defined by Myasnikov, Remeslennikov, and Serbin in [22] into $E(A, G)$. Moreover, we define the extension group $E(A, G)$ for arbitrary groups G and not only for free groups as done in previous work. We show some structural results about the group (existence and type of torsion elements, generation by elements of order 2) and we show that some interesting HNN extensions of G embed naturally in the larger group $E(A, G)$.

1 Introduction

In this paper we construct an extension of a given group G by infinite non-Archimedean words. The construction is effective and gives a new uniform method to study various groups that "behave like G ": limits of G in the Gromov-Hausdorff topology, fully residually G groups, groups obtained from G by free constructions, etc. Infinite non-Archimedean words appeared first in [22] in connection with group actions on trees. The fundamentals for group actions on simplicial trees (now known as Bass-Serre theory) were laid down by Serre in his seminal book [28].

*Part of the work has been started in 2007 when the authors where at the CRM (Centro Recherche Matemàtica, Barcelona). It was finished when the first author stayed at Stevens Institute of Technology in September 2010. The support of both institutions is greatly acknowledged

General Λ -trees for ordered abelian groups Λ were introduced by Morgan and Shalen in [21] and their theory was further developed by Alperin and Bass in [1]. The Archimedean case concerns with group actions on \mathbb{R} -trees.

A complete description of finitely generated groups acting freely on \mathbb{R} -trees was obtained in a series of papers [3, 9]. It is known now as Rips' Theorem, see [5] for a detailed discussion.

For non-Archimedean actions much less is known. Much of the recent progress is due to Chiswell and Müller [6], Kharlampovich, Myasnikov, Remeslennikov, and Serbin [16, 15, 22] and the recent thesis of Nikolaev [23]. In these papers groups acting on freely on \mathbb{Z}^n -trees are represented as words where the length takes values in the ring of integer polynomials $\mathbb{Z}[t]$. More precisely, in [22] the authors represent elements of Lyndon's free $\mathbb{Z}[t]$ -group $F^{\mathbb{Z}[t]}$ (the free group with basis Σ and exponentiation in $\mathbb{Z}[t]$) by infinite words, which are defined as mappings $w : [1, \alpha] \rightarrow \Sigma^{\pm 1}$ over closed intervals $[1, \alpha] = \{\beta \in \mathbb{Z}[t] \mid 1 \leq \beta \leq \alpha\}$. Here, the ring $\mathbb{Z}[t]$ is viewed as an ordered abelian group in the standard way: $0 < \alpha$ if the leading coefficient of the polynomial α is positive. This yields a regular free Lyndon length function with values in $\mathbb{Z}[t]$.

The importance of Lyndon's group $F^{\mathbb{Z}[t]}$ became also prominent due to its relation to algebraic geometry over groups and the solution of the Tarski Problems [11, 12, 13, 14]. It was known by [8] and the results above that finitely generated fully residually free groups are embeddable into $F^{\mathbb{Z}[t]}$. The converse (every finitely generated subgroup of $F^{\mathbb{Z}[t]}$ is fully residually free) was shown in the original paper by Lyndon [17]. It follows that every finitely generated fully residually free group has a free length function with values in a free abelian group of finite rank with the lexicographic order. It turned out that the representation of group elements as infinite words over $\mathbb{Z}[t]$ is quite intuitive and it enables a *combinatorics on words* similar to finite words. This technique leads to the solution of various algorithmic problems for $F^{\mathbb{Z}[t]}$ using the standard Nielsen cancellation argument for the length function.

This concept is the starting point for our paper: We use finite words over $\Sigma^{\pm 1}$ to represent elements of G . Then, exactly as in the earlier papers mentioned above, an infinite word is a mapping $w : [1, \alpha] \rightarrow \Sigma^{\pm 1}$ over a closed interval $[1, \alpha] = \{\beta \in \mathbb{Z}[t] \mid 1 \leq \beta \leq \alpha\}$. The monoid of infinite words is endowed with a natural involution. We can read $w : [1, \alpha] \rightarrow \Sigma^{\pm 1}$ from right-to-left and simultaneously we inverse each letter. This defines \bar{w} . Clearly, $\bar{\bar{w}} = w$ and $\overline{uv} = \bar{v}\bar{u}$. The naive idea is to use now $w\bar{w} = 1$ as defining relations in order to obtain a group. This idea falls short drastically, because the group collapses. The image of the $F(\Sigma)$ in this group is $\mathbb{Z}/2\mathbb{Z}$ (for $\Sigma \neq \emptyset$). Therefore the set of infinite words was viewed as a partial monoid, only. It was shown that $F^{\mathbb{Z}[t]}$ embeds into this partial monoid, but the proof is complicated and demands technical tools.

The first major deviation in our approach (from what has been done so far) is

that we still work with equations $w\bar{w} = 1$, but we restrict them to freely reduced words w . Just as in the finite case: A word w is called freely reduced, if no factor aa^{-1} (where a is a letter) appears. This means, there is no $1 < \beta < \alpha$ such that $w(\beta) = w(\beta + 1)^{-1}$. The submonoid generated by freely reduced words (inside the monoid of all infinite words) modulo defining equations $w\bar{w} = 1$ defines a group (which is trivial) where $F(\Sigma)$ embeds (which is non-trivial). Actually, $F^{\mathbb{Z}[t]}$ embeds. It turns out that many freely reduced words satisfy $\bar{w} = w$. Thus, the involution has fixed points, and many elements have 2-torsion in our group. Actually, in natural situations the group is generated by these elements of order 2.

Our focus is more ambitious and goes beyond extending free groups $F(\Sigma)$. We begin with an arbitrary group G generated by Σ . This gives rise to the notion of a G -reduced word. An $\mathbb{Z}[t]$ -word is G -reduced, if no finite factor $w[\beta, \beta + m]$ with $m \in \mathbb{N}$ represents the unit element 1 in G . We let $R^*(A, G)$ denote the submonoid generated by G -reduced words (inside the monoid of all infinite words) where $A = \mathbb{Z}[t]$. Clearly, we may assume that $R^*(A, G)$ contains all finite words (because we may assume that all letters are G -reduced). Then we factor out defining equations for G (which are words in $\Sigma^{\pm 1}$) and defining equations $u\bar{u} = 1$ with $u \in R^*(A, G)$. In this way we obtain a group denoted here by $E(A, G)$.

The first main result of the paper states that G embeds into $E(A, G)$, see Corollary 5.5. The result is obtained by the proof that some (non-terminating) rewriting system is strongly confluent, thus confluent. This is technically involved and covers all of Section 5.

The second main result concerns the question when the Word Problem is decidable in all finitely generated subgroups of $E(A, G)$. An obvious precondition is that the base group G itself must share this property. However, this is not enough and makes the situation somehow non-trivial. We show in Corollary 8.5 that the Word Problem is decidable in all finitely generated subgroups of $E(A, G)$ if and only if the Cyclic Membership Problem " $u \in \langle v \rangle$?" is decidable for all $v \in G$. There are known examples where G has a soluble Word Problem, but Cyclic Membership Problem is not decidable for some specific v , see [24, 25]. On the other hand, the Cyclic Membership Problem is uniformly decidable in many natural classes (which encompasses classes of groups with decidable Membership Problem w.r.t. subgroups) like hyperbolic groups, one-relator groups or effective HNN-extensions, see Remark 8.8.

In the final section we show that the partial monoid $\text{CDR}(A, \Sigma)$ of infinite words with a cyclically reduced decompositions (c.f. [22]) embeds in our group $E(A, G)$, and we show that some interesting HNN extensions can be embedded into $E(A, G)$ as well which are not realizable inside the partial monoid $\text{CDR}(A, \Sigma)$, Proposition 9.4. In order to achieve this result we show that every cyclically G -reduced word in $E(A, G)$ sits inside a free abelian subgroup of infinite rank, Proposition 9.3.

The proof techniques in this paper are of combinatorial flavor and rely on the theory of rewriting systems. No particular knowledge on non-Archimedean words or groups acting on \mathbb{Z}^n -trees is required.

2 Preliminaries on rewriting techniques

Rewriting techniques are a convenient tool to prove that certain constructions have the expected properties. Typically we extend a given group by new generators and defining equations and we want that the original group embeds in the resulting quotient structure. For example, HNN extensions and amalgamated products or Stallings's embedding (see [29]) of a pregroup in its universal group can be viewed from this viewpoint, [7]. Here we use them in the very same spirit. First, we recall the basic concepts.

A *rewriting relation* over a set X is binary a relation $\Longrightarrow \subseteq X \times X$. By $\xRightarrow{+}$ ($\xRightarrow{*}$ resp.) we mean the transitive (reflexive and transitive resp.) closure of \Longrightarrow . By $\xLeftrightarrow{*}$ ($\xLeftrightarrow{*}$ resp.) we mean the symmetric (symmetric, reflexive, and transitive resp.) closure of \Longrightarrow . We also write $y \xLeftarrow{*} x$ whenever $x \xRightarrow{*} y$, and we write $x \xRightarrow{\leq k} y$ whenever we can reach y in at most k steps from x .

Definition 2.1. *The relation $\Longrightarrow \subseteq X \times X$ is called:*

- i.) *strongly confluent, if $y \xLeftarrow{*} x \xRightarrow{*} z$ implies $y \xRightarrow{\leq 1} w \xLeftrightarrow{\leq 1} z$ for some w ,*
- ii.) *confluent, if $y \xLeftarrow{*} x \xRightarrow{*} z$ implies $y \xRightarrow{*} w \xLeftarrow{*} z$ for some w ,*
- iii.) *Church-Rosser, if $y \xLeftrightarrow{*} z$ implies $y \xRightarrow{*} w \xLeftarrow{*} z$ for some w ,*
- iv.) *locally confluent, if $y \xLeftarrow{*} x \xRightarrow{*} z$ implies $y \xRightarrow{*} w \xLeftarrow{*} z$ for some w ,*
- v.) *terminating, if every infinite chain*

$$x_0 \xRightarrow{*} x_1 \xRightarrow{*} \cdots x_{i-1} \xRightarrow{*} x_i \xRightarrow{*} \cdots$$

becomes stationary,

- vi.) *convergent (or complete), if it is locally confluent and terminating.*

The following facts are well-known, proofs are easy and can be found in any text book on rewriting systems, see e.g. [4, 10].

Proposition 2.2. *The following assertions hold:*

1. *Strong confluence implies confluence.*
2. *Confluence is equivalent with Church-Rosser.*
3. *Confluence implies local confluence, but the converse is false, in general.*
4. *Convergence (i.e., local confluence and termination together) implies confluence.*

Often one is interested in the case, only where X is a free group or a free monoid and the rewriting relation is specified by directing defining equations. Here we are more general in the following sense. Let M be any monoid. A *rewriting system* over M is a relation $S \subseteq M \times M$. Elements $(\ell, r) \in S$ are also called *rules*. The system S defines the rewriting relation $\xRightarrow[S]{*} \subseteq M \times M$ by

$$x \xRightarrow[S]{*} y, \text{ if } x = p\ell q, y = prq \text{ for some rule } (\ell, r) \in S.$$

The relation $\xRightarrow[S]{*} \subseteq M \times M$ is a congruence, hence the congruence classes form a monoid which is denoted by $M / \{\ell = r \mid (\ell, r) \in S\}$. Frequently we simply write M/S for this quotient monoid. Notice, that if M is a free monoid with basis X then M/S is the monoid given by the presentation $\langle X \mid \ell = r, \text{ where } (\ell, r) \in S \rangle$.

We say that S is strongly confluent or confluent etc, if in fact $\xRightarrow[S]{*}$ has the corresponding property. Instead of $(\ell, r) \in S$ we also write $\ell \rightarrow_S r \in S$ and $\ell \leftarrow_S r \in S$ in order to indicate that both $(\ell, r) \in S$ and $(r, \ell) \in S$. By $\text{IRR}(S)$ we mean the set of *irreducible normal forms*. This is the subset of M where no rule of S can be applied, i.e.,

$$\text{IRR}(S) = M \setminus \bigcup_{(\ell, r) \in S} M\ell M.$$

If S is terminating, then we have $1 \in \text{IRR}(S)$, and if S is convergent, then the canonical homomorphism $M \rightarrow M/S$ induces a bijection between $\text{IRR}(S)$ and the quotient monoid M/S .

If a quotient monoid is given by a finite convergent string rewriting system $S \subseteq \Gamma^* \times \Gamma^*$, then the monoid has a decidable Word Problem, which yields a major interest in these systems.

Example 2.3. *Let Σ be a set and Σ^{-1} be disjoint copy. Then the set of rules $\{aa^{-1} \rightarrow 1, a^{-1}a \rightarrow 1 \mid a \in \Sigma\}$ defines a strongly confluent and terminating system over $(\Sigma \cup \Sigma^{-1})^*$ which defines the free group $F(\Sigma)$ with basis Σ .*

In this paper however, we will deal mainly with non-terminating systems which are moreover in many cases infinite. So convergence plays a minor role here. There is another class of string rewriting systems which for finite systems leads to a polynomial space (and hence exponential time in the worst case) decision algorithm for the Word Problem.

Definition 2.4. A string rewriting system $S \subseteq \Gamma^* \times \Gamma^*$ is called pre-perfect, if the following three conditions hold:

1. The system S is confluent.
2. If we have $\ell \rightarrow r \in S$, then we have $|\ell| \geq |r|$ where $|x|$ denotes the length of a word x .
3. If we have $\ell \rightarrow r \in S$ with $|\ell| = |r|$, then we have $r \rightarrow \ell \in S$, too.

Clearly, a convergent length-reducing system is pre-perfect, and if a confluent system satisfies $|\ell| \geq |r|$ for all $\ell \rightarrow r \in S$, then we can add symmetric rules in order to make it pre-perfect.

3 Non-Archimedean words

We consider group extensions over infinite words of a specific type. These words are also called *non-Archimedean words*, because they are defined over non-archimedean ordered abelian groups.

3.1 Discretely ordered abelian groups

A *ordered abelian group* is an abelian group A together with a linear order \leq such that $x \leq y$ if and only if $x + z \leq y + z$ for all $x, y, z \in A$. It is *discretely ordered*, if in addition there is least positive element 1_A . Here, as usual, an element x is *positive*, if $0 < x$. An ordered abelian group is *Archimedean*, if for all $0 \leq a \leq b$ there is some $n \in \mathbb{N}$ such that $b < na$, otherwise it is *non-Archimedean*.

If B is any ordered abelian group, then $A = \mathbb{Z} \times B$ is discretely ordered with $1_A = (1, 0)$ and the lexicographical ordering:

$$(a, b) \leq (c, d) \text{ if } b < d \text{ or } b = d \text{ and } a \leq c.$$

The group is non-Archimedean unless B is trivial since $(n, 0) < (0, x)$ for all $n \in \mathbb{N}$ and positive $x \in B$.

In particular, $\mathbb{Z} \times \mathbb{Z}$ is a non-Archimedean discretely ordered abelian group. It serves as our main example. Iterating the process all finitely generated free

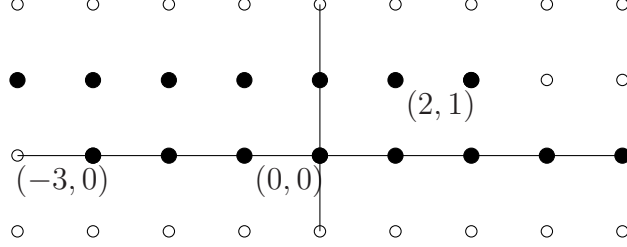


Figure 1: A closed interval of length $(6, 1)$ in $\mathbb{Z} \times \mathbb{Z}$

abelian \mathbb{Z}^k are viewed as being discretely ordered; and by a transfinite iteration we can consider arbitrary direct sums of \mathbb{Z} . This is where we limit ourselves. In this paper we consider discretely ordered abelian groups only, which can be written as

$$A = \oplus_{i \in \Omega} \langle t_i \rangle, \quad (1)$$

where Ω is a set of ordinals, and $\langle t_i \rangle$ denotes the infinite cyclic group \mathbb{Z} generated by the element t_i . Elements of A are finite sums $\alpha = \sum_i n_i t_i$ with $n_i \in \mathbb{Z}$. Since the sum is finite, either $\alpha = 0$ or there is a greatest ordinal $i \in \Omega$ (denoted by $\deg(\alpha)$) with $n_i \neq 0$. By convention, $\deg(0) = -\infty$. We call $\deg(\alpha)$ the *degree* or *height* of α . An element $\alpha = \sum_i n_i t_i \in A$ is called *positive*, if $n_d > 0$ for $d = \deg(\alpha)$. We let $\alpha \leq \beta$, if $\alpha = \beta$ or $\beta - \alpha$ is positive. Moreover, for $\alpha, \beta \in A$ we define the *closed interval* $[\alpha, \beta] = \{\gamma \in A \mid \alpha \leq \gamma \leq \beta\}$. Its *length* is defined to be $\beta - \alpha + 1$.

For $\mathbb{Z} \times \mathbb{Z}$ the interval $[(-3, 0), (2, 1)]$ is depicted as in Fig. 1. Its length is $(6, 1)$.

Sometimes we simply illustrate intervals of length $(m, 1)$ as \dots and intervals of length $(m, 2)$ as $\dots(\dots)$. This will become clearer later.

3.2 Non-Archimedean words over a group G

An *involution* of a set M is a mapping $M \rightarrow M, x \mapsto \bar{x}$ with $\bar{\bar{x}} = x$ for all $x \in M$. A *monoid with involution* is a monoid M with an involution $x \mapsto \bar{x}$ such that $\overline{xy} = \bar{y}\bar{x}$ for all $x, y \in M$ and, as a consequence, $\bar{1} = 1$. Every group is a monoid with involution $x \mapsto x^{-1}$. Obviously, if M is a monoid with involution $x \mapsto \bar{x}$ then the quotient $M / \{x\bar{x} = 1 \mid x \in M\}$ is a group. Furthermore, if G is a group and M is a monoid with involution then every monoid homomorphism respecting involutions $\varphi : M \rightarrow G$ factors through this canonical quotient. Let

$a \mapsto \bar{a}$ denote a bijection between sets Σ and $\bar{\Sigma}$, hence $\bar{\Sigma} = \{\bar{a} \mid a \in \Sigma\}$. The map $a \mapsto \bar{a}, \bar{a} \mapsto a$ is an involution on $\Sigma \cup \bar{\Sigma}$ with $\bar{\bar{a}} = a$. It extends to an involution $x \mapsto \bar{x}$ on the free monoid $(\Sigma \cup \bar{\Sigma})^*$ with basis $\Sigma \cup \bar{\Sigma}$ by $\overline{a_1 \cdots a_n} = \bar{a}_n \cdots \bar{a}_1$. In case that $\Sigma \cap \bar{\Sigma} = \emptyset$ the resulting structure $((\Sigma \cup \bar{\Sigma})^*, \cdot, 1, \bar{\cdot})$ is the *free monoid with involution* with basis Σ .

Throughout G denotes a group with a generating set Σ . We always assume that $a \neq 1$ for all $a \in \Sigma$. We let $\Gamma = \Sigma \cup \bar{\Sigma}$, where $\bar{\Sigma} = \Sigma^{-1} \subseteq G$ and $\bar{a} = a^{-1}$ for $a \in \Gamma$. The inclusion $\Gamma \subseteq G$ induces the canonical homomorphism (presentation) onto the group G :

$$\pi : \Gamma^* \rightarrow G.$$

Clearly, for every word $w \in \Gamma^*$ we have $\pi(\bar{w}) = \pi(w)^{-1}$. Note that there are fixed points for the involution on Γ in case Σ contains an element of order 2.

Let $A = \oplus_{i \in \Omega} \langle t_i \rangle$ be a discretely ordered abelian group as above. A *partial A-map* is a map $p : D \rightarrow \Gamma$ with $D \subseteq A$. Two partial maps $p : D \rightarrow \Gamma$ and $p' : D' \rightarrow \Gamma$ are termed equivalent if p' is an α -shift of p for some $\alpha \in A$, i.e., $D' = \{\alpha + \beta \mid \beta \in D\}$ and $p'(\alpha + \beta) = p(\beta)$ for all $\beta \in D$. This an equivalence relation on partial A -maps, and an equivalence class of partial A -maps is called a *partial A-word*. If $D = [\alpha, \beta] = \{\gamma \in A \mid \alpha \leq \gamma \leq \beta\}$ then the equivalence class of $p : [\alpha, \beta] \rightarrow \Gamma$ is called a *closed A-word*. By abuse of language a closed (resp. partial) A -word is sometimes simply called a *word* (resp. *partial word*).

A word $p : [\alpha, \beta] \rightarrow \Gamma$ is *finite* if the set $[\alpha, \beta]$ is finite, otherwise it is *infinite*. Usually, we identify finite words with the corresponding elements in Γ^* .

If $p : [\alpha, \beta] \rightarrow \Gamma$ and $q : [\gamma, \delta] \rightarrow \Gamma$ are closed A -words, then we define their concatenation as follows. We may assume that $\gamma = \beta + 1$ and we let:

$$\begin{aligned} p \cdot q : [\alpha, \delta] &\rightarrow \Gamma \\ x &\mapsto p(x) && \text{if } x \leq \beta \\ x &\mapsto q(x) && \text{otherwise.} \end{aligned}$$

It is clear that this operation is associative. Hence, the set of closed A -words forms a monoid, which we denote by $W(A, \Gamma)$. The neutral element, denoted by 1, is the totally undefined mapping. The standard representation of an A -word p is a mapping $p : [1, \alpha] \rightarrow \Gamma$, where $0 \leq \alpha$. In this case α is called the *length* of p ; sometimes we also write $|p| = \alpha$. The *height* or *degree* of p is the degree of α ; we also write $\deg(p) = \deg(\alpha)$. For a partial word $p : D \rightarrow \Gamma$ and $[\alpha, \beta] \subseteq D$ we denote by $p[\alpha, \beta]$ the restriction of p to the interval $[\alpha, \beta]$. Hence $p[\alpha, \beta]$ is a closed word. Sometimes we write $p[\alpha]$ instead of $p[\alpha, \alpha]$. Thus, $p[\alpha] = p(\alpha)$.

The monoid $W(A, \Gamma)$ is a monoid with involution $p \mapsto \bar{p}$ where for $p : [1, \alpha] \rightarrow \Gamma$ we define $\bar{p} \in W(A, \Gamma)$ by $\bar{p} : [-\alpha, -1] \rightarrow \Gamma, -\beta \mapsto p(\beta)$.

Recall that $A = \oplus_{i \in \Omega} \langle t_i \rangle$. We may assume that 0 is the least ordinal in Ω , in which case \mathbb{Z} can be viewed as a subgroup of A via the embedding $n \mapsto nt_0$. Thus $1 \in \mathbb{N}$ is also the smallest positive element in A . If, for example, $A = \mathbb{Z} \times \mathbb{Z}$, then we have identified $1 \in \mathbb{N}$ with the pair $(1, 0)$.

If $x \in W(A, \Gamma)$ and $x = pfq$ for some $p, q \in W(A, \Gamma)$ then p is called a *prefix*, q is called a *suffix*, and f is called a *factor* of x . If $1 \neq f \neq x$ then f is called a *proper factor*. As usual, a factor is finite, if $|f| \in \mathbb{N}$. Thus, a finite factor can be written as $x[\alpha, \beta]$ where $\beta = \alpha + n$, $n \in \mathbb{N}$.

A closed word $x : [1, \alpha] \rightarrow \Gamma$ is called *freely reduced* if $x(\beta) \neq \overline{x(\beta + 1)}$ for all $1 \leq \beta < \alpha$. It is called *cyclically reduced* if x^2 is freely reduced.

As a matter of fact we need a stronger conditions. The word x is called *G-reduced*, if no finite factor $x[\alpha, \alpha + n]$ with $n \in \mathbb{N}$, $n \geq 1$, becomes the identity 1 in the group G . Note that all *G-reduced* words are freely reduced by definition. We say x is *cyclically G-reduced*, if every finite power x^k with $k \in \mathbb{N}$ is *G-reduced*. Over a free group G with basis Σ a word is freely reduced if and only if it is *G-reduced*, and it is cyclically *G-reduced* if and only if it is cyclically reduced.

In Fig. 2 we see a closed word which is not freely reduced. Fig. 3 defines a word w with a sloppy notation $[aaa \cdots)(\cdots abab \cdots)(\cdots bbb]$. Fig. 4 shows that for the same word w we have $aw \neq wb$ (because $aw[(0, 1)] = a$ and $wb[(0, 1)] = b$), but we have $aaw = wbb$ in the monoid $W(A, \Gamma)$, see Fig. 5. Recall, that two elements x, y in a monoid M are called *conjugated*, if $xw = wy$ for some $w \in M$. Fig. 6 shows that all finite words $x, y \in \Gamma^*$ are conjugated in $W(A, \Gamma)$ provided they have the same length $|x| = |y|$ and A is non-Archimedean. Indeed $t = [uuu \cdots)(\cdots vvv]$ does the job $ut = tv$. Clearly, $ut = tv$ implies $|x| = |y|$. In particular, this shows that the monoid $W(A, \Gamma)$ is not free. Indeed, if x and y are conjugated elements in a free monoid, say $xw = wy$, then $x = rs$, $y = sr$, and $w = (rs)^m r$ for some $r, s \in \Gamma^*$ and $m \in \mathbb{N}$, which is not the case for the example above.

If G is an infinite group, then there are *G-reduced* A -words of arbitrary length.

Lemma 3.1. *Let G be an infinite group and $\alpha \in A$. Then there exists a *G-reduced* A -word $x : [1, \alpha] \rightarrow \Gamma$ of length α .*

Proof. First, let us assume that Γ is finite. We may assume that letters of Γ are *G-reduced*. There are infinitely many finite *G-reduced* words in Γ^* , simply because each group element can be represented this way. They form a tree in the following way. The root is the empty word 1. A letter has 1 as its parent node. A finite *G-reduced* word of the form $w = avb$ with $a, b \in \Gamma$ has v as its parent node. Since Γ is finite the degree of each node is finite. Hence König's Lemma tells us that there must be an infinite path. Following this path from the root yields a partial word $p : \mathbb{Z} \rightarrow \Gamma$ in an obvious way: If v denotes the *G-reduced* word $v : [m, n] \rightarrow \Gamma$, then $w = avb$ denotes the *G-reduced* word $w : [m - 1, n + 1] \rightarrow \Gamma$

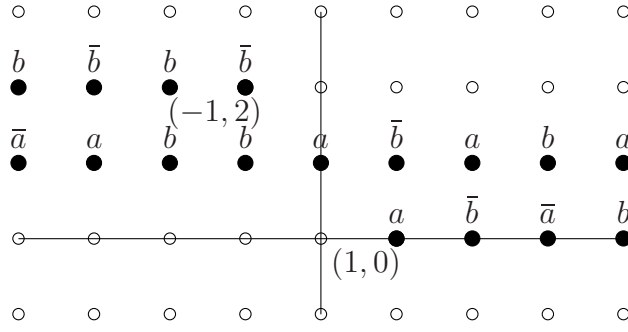


Figure 2: A closed non-freely reduced word of length $(-1, 2)$.

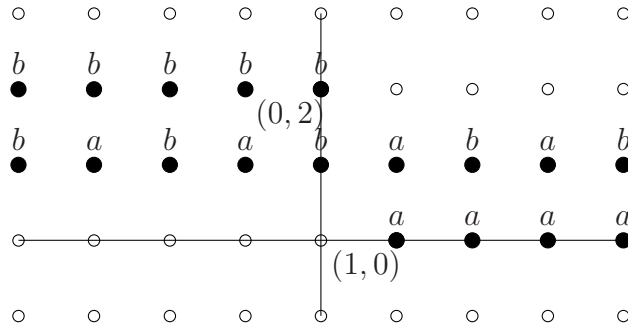


Figure 3: A word w representing $[aaa \dots](\dots abab \dots)(\dots bbb)$

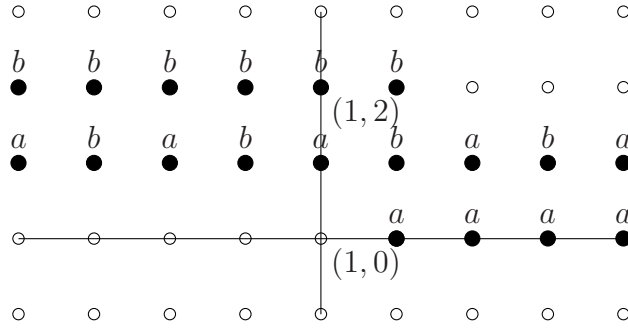


Figure 4: $aw = a[aaa \dots](\dots abab \dots)(\dots bbb)$ and $aw \neq wb$.

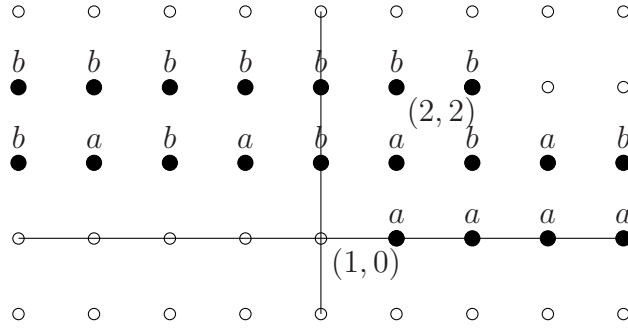


Figure 5: $aa[aaa \dots](\dots abab \dots)(\dots bbb)bb = [aaa \dots](\dots abab \dots)(\dots bbb)bb$

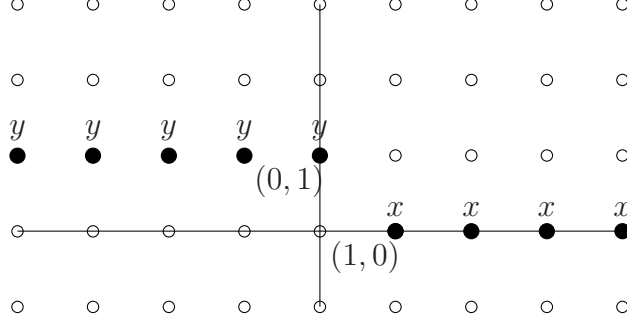


Figure 6: An infinite word $t = [xxx \cdots](\cdots yyy]$ where $xt = ty$.

with $w[m-1] = a$, $w[m, n] = v$, and $w[n+1] = b$. This mapping $p : \mathbb{Z} \rightarrow \Gamma$ can be extended to a mapping $q : A \rightarrow \Gamma$ by $q(\sum_i n_i t_i) = p(n_0)$. This means we project $\alpha \in A$ to the first component and then we use p . For every $\alpha \in A$ the partial word $q[1, \alpha] \rightarrow \Gamma$ is G -reduced.

If G is finitely generated but Γ is infinite then one can repeat the argument above for some large enough finite subset of Γ (that generates G). It remains to consider the case that G is not finitely generated. Assume a G -reduced word $v : [m, n] \rightarrow \Gamma$ has been constructed. Then we choose $a \in \Gamma$ such that a is not in subgroup generated by the elements $v[i]$ for $m \leq i \leq n$. Clearly, $av : [m-1, n] \rightarrow \Gamma$ is G -reduced. Next choose $b \in \Gamma$ such that b is not in subgroup generated by the elements $av[i]$ for $m-1 \leq i \leq n$. Now, $avb : [m-1, n+1] \rightarrow \Gamma$ is G -reduced. We obtain a G -reduced word $p : \mathbb{Z} \rightarrow \Gamma$ and we argue as above. \square

By $R(A, G)$ we denote the set of all G -reduced words in $W(A, \Gamma)$, and by $R^*(A, G)$ we mean the submonoid of $W(A, \Gamma)$ which is generated by $R(A, G)$.

Remark 3.2. *In the notation above:*

- If the group G is finite, then $R(A, G)$ cannot contain any infinite word, and in this case $R^*(A, G) = \Gamma^*$.
- If $A = \mathbb{Z}$ then $W(\mathbb{Z}, \Gamma) = \Gamma^*$.

These situations are without any interest in our context, so we assume in the sequel that G is infinite and that A has rank at least 2 (i.e., it is non-Archimedean).

Observe, that the length function $W(A, \Gamma) \rightarrow A, p \mapsto |p|$ induces a canonical homomorphism onto $\oplus_{i \in \Omega} \mathbb{Z}/2\mathbb{Z}$ which therefore factors through the greatest

quotient group of $W(A, \Gamma)$. This group collapses Σ into a group of order 2, and therefore the greatest quotient group of $W(A, \Gamma)$ is of no particular interest here. More precisely, we have the following fact.

Proposition 3.3. *Let $\Sigma \neq \emptyset$ and*

$$\psi : F(\Sigma) \rightarrow W(A, \Gamma) / \{u\bar{u} = 1 \mid u \in W(A, \Gamma)\}$$

be the canonical homomorphism induced by $\Sigma \subseteq W(A, \Gamma)$, and let A have rank at least 2. Then the image of $F(\Sigma)$ under ψ is the group $\mathbb{Z}/2\mathbb{Z}$.

Proof. The image of $F(\Sigma)$ is not trivial, because it is non-trivial in the group $\oplus_{i \in \Omega} \mathbb{Z}/2\mathbb{Z}$. It is therefore enough to show that $\psi(ab) = 1$ for all $a, b \in \Gamma$. Consider the following closed word u of length $(0, 1)$:

$$u = [ababab \cdots](\cdots a\bar{a}a\bar{a}a\bar{a})$$

In $W(A, \Gamma)$ we have $abu = ua\bar{a}$. Now, $\psi(a\bar{a}) = 1$ implies $\psi(ab) = 1$. \square

Continuing with $F(\Sigma)$, consider the following word w of length $(0, 2)$, which is product of two freely reduced words where $a, b \in \Gamma$ with $a \neq \bar{b}$:

$$w = [aaa \cdots](\cdots aaa) \cdot [\bar{a}\bar{a}\bar{a} \cdots](\cdots bbb)$$

It is natural to allow (and we will do) the cancellation of factors $a\bar{a}$ inside w . The shape of the word remains the same, but the length is decreasing to any value $(-2n, 2)$ with $n \in \mathbb{N}$. If next we wish to embed $F(\Sigma)$ into any quotient structure of $W(A, \Gamma)$, then we cannot cancel however the whole middle part $(\cdots aaa) \cdot [\bar{a}\bar{a}\bar{a} \cdots]$, i.e., w cannot become equal to $v = [aaa \cdots](\cdots bbb)$ in this quotient. Indeed, assume by contradiction $w = v$, then:

$$\begin{aligned} aav = avb &= a[aaa \cdots](\cdots bbb)b \\ &= awb \\ &= [aaa \cdots](\cdots aaa) \cdot a\bar{a} \cdot [\bar{a}\bar{a}\bar{a} \cdots](\cdots bbb) \\ &= w = v. \end{aligned}$$

This implies $a^2 = 1$, a contradiction.

4 The group $E(A, G)$

Proposition 3.3 shows that, in general, the free group $F(\Sigma)$ does not naturally embed into the greatest quotient group of $W(A, \Gamma)$. Nevertheless, in this section we modify the construction to be able to represent a group G by infinite words

from $W(A, \Gamma)$. As above, we let G be a group generated by Σ and $\pi : \Gamma^* \rightarrow G$ be the induced presentation with $\Gamma = \Sigma \cup \Sigma^{-1}$. Recall that $R(A, G)$ denotes the set of closed G -reduced words, i.e.:

$$R(A, G) = \{u \in W(A, \Gamma) \mid u \text{ is } G\text{-reduced}\}.$$

Let $\mathcal{M}(A, G)$ be the following quotient monoid of $W(A, \Gamma)$:

$$\mathcal{M}(A, G) = W(A, \Gamma) / \{u\ell\bar{r}\bar{u} = 1 \mid u \in R(A, G), \ell, r \in \Gamma^*, \pi(\ell) = \pi(r)\}.$$

Definition 4.1. We define $E(A, G)$ as the image of $R^*(A, G)$ in $\mathcal{M}(A, G)$ under the canonical epimorphism $W(A, \Gamma) \rightarrow \mathcal{M}(A, G)$.

In the following proposition we collect some simple results on $E(A, G)$.

Proposition 4.2. Let G be a group generated by a set Σ and $A = \bigoplus_{i \in \Omega} \langle t_i \rangle$ as above. Then:

- 1) $E(A, G)$ is a group (a subgroup of $\mathcal{M}(A, G)$);
- 2) every submonoid of $\mathcal{M}(A, G)$ which is a group sits inside the group $E(A, G)$, so $E(A, G)$ is the group of units in $\mathcal{M}(A, G)$;
- 3) the inclusion $\Gamma \subseteq G$ induces a homomorphism $\pi^A : G \rightarrow E(A, G)$.

Proof. To see 1) observe that every element in $u \in R(A, G)$ has \bar{u} as an inverse in $E(A, G)$, so $E(A, G)$ is a group.

Notice that only the trivial word is invertible in $W(A, \Gamma)$ since concatenation does not decrease the length. Hence every equality $w\bar{w} = 1$ for a non-trivial w in $W(A, \Gamma)$ comes from the defining relations in $\mathcal{M}(A, G)$. Observe, that the defining relations are applicable only to words from $R^*(A, G)$, the set $R^*(A, G)$ is closed under such transformations. This shows that $E(A, G)$ is the group of units in $\mathcal{M}(A, G)$, as claimed in 2).

3) is obvious since $G = \Gamma^* / \{\ell\bar{r} = 1 \mid \pi(\ell) = \pi(r)\}$ and $1 \in R(A, G)$. \square

Several important remarks are due here.

- It is far from obvious that the homomorphism $\pi^A : G \rightarrow E(A, G)$ is injective. However, this is true and we prove it later in Corollary 5.5.
- It is not claimed that the definition of $\mathcal{M}(A, G)$ (or $E(A, G)$) is independent of the choice of Γ and π , but our main results hold through for any such Γ and π thus justifying the (sloppy) notations $\mathcal{M}(A, G)$ and $E(A, G)$.

- If $G = F(\Sigma)$ is the free group with basis Σ , then the definition of $\mathcal{M}(A, G)$ can be rephrased by saying that it is the quotient monoid of $W(A, \Gamma)$ with defining equations $u\bar{u} = 1$ for all freely reduced closed words u .
- It is not true in general that $E(A, G)$ can be defined as the quotient group

$$E(A, F(\Sigma)) / \{ \ell = r \mid \ell, r \in \Gamma^*, \pi(\ell) = \pi(r) \}.$$

Indeed, let r be a cyclically reduced word of length m such that $r = 1$ in G . In $E(A, F(\Sigma))$ for every $a \in \Gamma$ the words a^m and r are conjugated since

$$a^m [a^m a^m a^m \dots] (\dots rrr) = [a^m a^m a^m \dots] (\dots rrr) r.$$

Therefore, $a^m = 1$ in $E(A, F(\Sigma)) / \{ \ell = r \mid \ell, r \in \Gamma^*, \pi(\ell) = \pi(r) \}$, which may not be the case in G (which is a subgroup of $E(A, G)$).

Nevertheless, $E(A, F(\Sigma))$ satisfies some universal property.

Proposition 4.3. *Every group G generated by Σ is isomorphic to the canonical quotient of the subgroup in $E(A, F(\Sigma))$ generated by $R(A, G)$.*

Proof. The statement is obvious. □

5 Confluent rewriting systems over non-Archimedean words

Our goal here is to construct a confluent rewriting system S over the monoid $W(A, \Gamma)$ such that

$$\mathcal{M}(A, G) = W(A, \Gamma) / S$$

and S has the following form:

$$S = S_0 \cup \{ u\bar{u} \rightarrow 1 \mid u \in R(A, G) \text{ and } u \text{ is infinite} \}, \quad (2)$$

where $S_0 \subseteq \Gamma^* \times \Gamma^*$ is a rewriting system for G satisfying the following conditions:

1. $\Gamma^* / S_0 = G$
2. For all $a \in \Gamma$ we have $(a\bar{a}, 1) \in S_0$.
3. If $(\ell, r) \in S_0$, then $(\bar{\ell}, \bar{r}) \in S_0$.
4. $1 \in \Gamma^*$ is S_0 -irreducible.

5. S_0 is confluent.

In general, S_0 is neither finite nor terminating, but these conditions are not crucial for the moment, so we do not care.

Lemma 5.1. *For any group G generated by Σ there is a rewriting system $S_0 \subseteq \Gamma^* \times \Gamma^*$ satisfying the condition 1-5 above. Moreover, if G is finitely presented, then one can choose S_0 to be finite.*

Proof. Let $G = \Gamma^*/R$ for some set of defining relation R . In general, let S_0 be the set of all rules $u \rightarrow v$, where u is non-empty and $u \neq v$ as words, but $u = v$ in G . Notice that there are no rules $1 \rightarrow r$ in S_0 , so $1 \in IRR(S_0)$. However, for every $r \in R \cup \overline{R}$ and every letter $a \in \Sigma$ the relations $a \rightarrow ra$ and $a \rightarrow ar$ are in S_0 , so one can insert any relation r in a word, thus simulating the rule $1 \rightarrow r$.

In the case when R is finite consider only those rules $u \rightarrow v$ from S_0 such that $|u| + |v| \leq k + 2$, where $k = \max\{|\ell| + |r| \mid \ell \rightarrow r \in R\}$. Notice, again that all the rules of the type $a \rightarrow ra$ and $a \rightarrow ar$ are in S_0 . \square

Clearly:

$$M(A, \Gamma) = W(A, \Gamma)/S.$$

The following lemma will be used only later. The proof shows however our basic techniques to factorize and to reason about rewriting steps. The reader is therefore invited to read the proof carefully.

Lemma 5.2. *Let $x \in R(A, G)$ be a non-empty G -reduced word. Then $x \xrightarrow[S]{*} y$ implies both $x \xrightarrow[S_0]{*} y$ and y is a non-empty word.*

Proof. By contradiction, assume $x \xrightarrow[S]{*} y$, but not $x \xrightarrow[S_0]{*} y$. Then there are an infinite G -reduced word $u \in R(A, G)$ and some closed word y_0 such that $x \xrightarrow[S_0]{*} y_0 \xrightarrow[S]{*} y$ where the rule $u\bar{u} \rightarrow 1$ applies to y_0 . Note that rules of S_0 replace left-hand sides inside finite intervals. These intervals can be made larger and if two of them are separated by a finite distance, then we can join them. Hence we obtain a picture as follows where all x_i are infinite, and all f_i, g_i are finite words:

$$\begin{aligned} x &= x_1 f_1 \cdots x_{n-1} f_{n-1} x_n \\ y_0 &= x_1 g_1 \cdots x_{n-1} g_{n-1} x_n = p u \bar{u} q, \\ p q &\xrightarrow[S]{*} y, \\ f_i &\xrightarrow[S_0]{*} g_i \text{ for } 1 \leq i \leq n. \end{aligned}$$

The middle position of $y_0 = pu\bar{u}q$ between $u\bar{u}$ cannot be inside some factor x_m as x is G -reduced. The middle position meets therefore some finite factor g_m . Thus, (as u is infinite) we can enlarge f_m such that $f_m \xrightarrow[S_0]{*} 1$. This implies $f_m = g_m = 1$ as words, because x is G -reduced and 1 is irreducible w.r.t. S_0 . Let a be the last letter of u , then it is the last letter of x_m and \bar{a} is the first letter of x_{m+1} , too. Hence $a\bar{a}$ appears as a factor in x . This is a contradiction, and therefore $x \xrightarrow[S_0]{*} y$.

Since x is a non-empty G -reduced word, we cannot have both $x \xrightarrow[S_0]{*} y$ and $y = 1$. \square

The main technical result of this section is the following theorem.

Theorem 5.3. *The system $S \subseteq \Gamma^* \times \Gamma^* \cup R(A, G) \times R(A, G)$ defined in Equation 2 is confluent on $W(A, \Gamma)$.*

For technical reasons we replace the rewrite system $\xrightarrow[S]{*}$ by a new system which is denoted by $\xRightarrow[\text{Big}]{}$. It is defined by

$$\xRightarrow[\text{Big}]{} = \xrightarrow[S_0]{*} \circ \xrightarrow[S]{*} \circ \xrightarrow[S_0]{*}.$$

We have $x \xRightarrow[\text{Big}]{} y$ if and only if there is a derivation $x \xrightarrow[S]{+} y$ which may use many times rules from S_0 , but at most once a rule from the sub system

$$\{u\bar{u} \rightarrow 1 \mid u \in R(A, G) \text{ and } u \text{ is infinite}\}.$$

The notation is due to the fact that we can think of *Big* rules in this subsystem.

The proof of Theorem 5.3 is an easy consequence of the following lemma. However, the proof of this lemma is somehow tedious, technical, and rather long.

Lemma 5.4. *The rewriting system $\xRightarrow[\text{Big}]{}$ is strongly confluent on $W(A, \Gamma)$.*

Proof. We start with the situation

$$y \xleftarrow[\text{Big}]{} x \xrightarrow[\text{Big}]{} z,$$

and we have to show that there is some w with

$$y \xRightarrow[\text{Big}]{\leq 1} w \xleftarrow[\text{Big}]{\leq 1} z.$$

This is clear, if we have $y \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z$, because S_0 is confluent and several steps using $\xRightarrow[\text{Big}]{}$ yield at most one step in $\xRightarrow[\text{Big}]{}$.

Next, we consider the following situation

$$y \xleftarrow[S_0]{*} y_1 \xleftarrow[S]{} y_0 \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z.$$

We content to find a w such that

$$y_1 \xrightarrow[S_0]{*} w \xleftarrow[\text{Big}]{\leq 1} z.$$

Here comes a crucial observation which is used throughout in the following (compare to the proof of Lemma 5.2). We find factorizations as follows.

$$\begin{aligned} x &= f_0 x_1 f_1 \cdots x_n f_n \\ y_0 &= g_0 x_1 g_1 \cdots x_n g_n \\ z &= h_0 x_1 h_1 \cdots x_n h_n \end{aligned}$$

Moreover, all f_i are finite, all x_i are infinite, and always:

$$g_i \xleftarrow[S_0]{*} f_i \xrightarrow[S_0]{*} h_i.$$

In addition we may assume that $y_0 = pu\bar{u}q$ with $y_1 = pq$ and u is an infinite G -reduced word. We can shrink u by some finite amount and we can make all f_i larger and we can split some x_i into factors. As a consequence we may assume the left-hand side $u\bar{u}$ covers exactly some factor $x_\ell \cdots x_k$ for $1 \leq \ell \leq k \leq n$. In particular, we have

$$y_1 = g_0 x_1 g_1 \cdots x_{\ell-1} g_{\ell-1} g_{k+1} x_{k+1} x_n g_n.$$

Since S_0 is confluent, it is enough to consider the case $x = x_\ell \cdots x_k$. We may therefore simplify the notation and we assume the following:

$$\begin{aligned} x &= x_1 f_1 \cdots x_{n-1} f_{n-1} x_n \\ y_0 &= x_1 g_1 \cdots x_{n-1} g_{n-1} x_n = u\bar{u} \\ z &= x_1 h_1 \cdots x_{n-1} h_{n-1} x_n \\ y_1 &= 1 \end{aligned}$$

We may assume that the middle position between u and \bar{u} is inside some factor g_m . By making f_m larger we may assume that g_m has the form $g_m = r_m \overline{r_m}$. But then we have $h_m \xrightarrow[S_0]{*} 1$, and hence we may assume that $f_m = g_m = h_m = 1$. Refining the partition, making f_i larger, and shrinking u by some finite amount, we arrive at the following situation with $n = 2m$ and

$$y_0 = x_1 g_1 \cdots x_{m-1} g_{m-1} x_m \overline{x_m} \overline{g_{m-1}} \overline{x_{m-1}} \cdots \overline{g_1} \overline{x_1}$$

As $u = x_1 g_1 \cdots x_{m-1} g_{m-1} x_m$ we see that all x_i are G -reduced. For each $1 \leq i \leq m-1$ we find r_i such that $g_i \xrightarrow[S_0]{*} r_i$, $h_i \xrightarrow[S_0]{*} r_i$, and $h_{m+i} \xrightarrow[S_0]{*} \overline{r_{m-i}}$. As a consequence we may assume

$$z = x_1 r_1 \cdots x_{m-1} r_{m-1} x_m \overline{x_m} \overline{r_{m-1}} \overline{x_{m-1}} \cdots \overline{r_1} \overline{x_1}$$

Note that it is not clear that the word $x_1 r_1 \cdots x_{m-1} r_{m-1} x_m$ is G -reduced. So we start looking for a finite non-empty factor h with $h \xrightarrow[S_0]{*} 1$. If we find such a factor, we cancel it and we cancel the corresponding symmetric factor \bar{h} on the right side in $\overline{x_m} \overline{r_{m-1}} \overline{x_{m-1}} \cdots \overline{r_1} \overline{x_1}$. The factor must use a piece of some r_i because all x_i are G -reduced. But it never can use all of some r_i because $x_1 g_1 \cdots x_{m-1} g_{m-1} x_m$ is G -reduced. Thus, the cancellation process stops and we can replace z by some word which has the form $z = v\bar{v}$, where v is indeed G -reduced. Thus, the rewrite step $z \xRightarrow[\text{Big}]{*} 1$ finishes the situation

$$y \xleftarrow[S_0]{*} y_1 \xleftarrow[S]{} y_0 \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z.$$

For later use we recall that we found some w and derivation as follows:

$$y \xrightarrow[S_0]{*} w \xleftarrow[\text{Big}]{\leq 1} z.$$

The challenge is now to consider a situation as follows.

$$y \xleftarrow[S_0]{*} y_1 \xleftarrow[S]{} y_0 \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z_0 \xrightarrow[S]{} z_1 \xrightarrow[S_0]{*} z.$$

We claim that it is enough to find some w with

$$y_1 \xrightarrow[\text{Big}]{\leq 1} w \xleftarrow[\text{Big}]{\leq 1} z_1.$$

Indeed, if such a w exists, then we have just seen that there are w_1, w_2 with

$$y \xrightarrow[\text{Big}]{\leq 1} w_1 \xleftarrow[S_0]{*} w \xrightarrow[S_0]{*} w_2 \xleftarrow[\text{Big}]{\leq 1} z.$$

By confluence of S_0 there is some w' with

$$w_1 \xrightarrow[S_0]{*} w' \xleftarrow[S_0]{*} w_2.$$

We are done, because now

$$y \xrightarrow[\text{Big}]{\leq 1} w' \xleftarrow[\text{Big}]{\leq 1} z.$$

The claim now implies that we are left with the following case:

$$y \xleftarrow[S]{} y_0 \xleftarrow[S_0]^* x \xrightarrow[S_0]^* z_0 \xrightarrow[S]{} z.$$

We repeat the assumptions and notations from above. We have

$$\begin{aligned} x &= f_0 x_1 f_1 \cdots x_n f_n \\ y_0 &= g_0 x_1 g_1 \cdots x_n g_n \\ z_0 &= h_0 x_1 h_1 \cdots x_n h_n \end{aligned}$$

All f_i are finite, all x_i are infinite, and always:

$$g_i \xleftarrow[S_0]^* f_i \xrightarrow[S_0]^* h_i.$$

We may assume that $y_0 = Pu\bar{u}q$ and $z_0 = pv\bar{v}Q$ with $y_1 = Pq$ and $y_1 = pQ$ and u and v are infinite G -reduced words. We can shrink u and v by some finite amount and we can make all f_i larger and we can split some x_i . As a consequence we may assume the left-hand side $u\bar{u}$ covers exactly some factor $x_\ell \cdots x_k$ with $1 \leq \ell \leq k \leq n$, and the left-hand side $v\bar{v}$ covers exactly some factor $x_L \cdots x_K$ with $1 \leq L \leq K \leq n$. We say that g_i is covered by $u\bar{u}$, if $\ell \leq i < k$. If g_i is not covered, then we may assume that $g_i = f_i$. Analogously, h_i is covered by $v\bar{v}$, if $L \leq i < K$. If h_i is not covered, then we may assume that $h_i = f_i$.

We may assume that $\ell \leq L$. If there is no overlap between the factors $u\bar{u}$ and $v\bar{v}$, i.e., if $k < L$, then the situation is trivial, because those g_i or h_i which are not covered, are still equal to f_i . Thus, we have overlap. Moreover, we may assume that $f_0 = f_n = 1$, $\ell = 1$, and $n = \max\{k, K\}$. In order to clarify we repeat

$$\begin{aligned} x &= x_1 f_1 \cdots x_n \\ y_0 &= x_1 g_1 \cdots x_n = u\bar{u}q \\ z_0 &= x_1 h_1 \cdots x_n = pv\bar{v}Q \text{ and either } q = 1 \text{ or } Q = 1 \\ y &= x_{k+1} f_{k+1} \cdots x_{n-1} f_{n-1} x_n \\ z &= x_1 f_1 \cdots x_{L-1} f_{L-1} f_K x_{K+1} \cdots f_{n-1} x_n \end{aligned}$$

We are coming to a subtle point. As above we may assume that the middle position between $u\bar{u}$ is inside some g_m and and that the middle position between $v\bar{v}$ is inside some h_M . There are two cases $m = M$ or $m \neq M$. Let us treat the case $m = M$, first.

Given the preference to u we may enlarge f_m such that $g_m = r\bar{r}$. Thus, actually we may assume $g_m = 1$. However it is not clear that h_m can be factorized the same way. But h_m is finite and v is infinite, hence, by left-right symmetry, we have $h_m = s\bar{s}h$, where $\bar{s}h$ is a prefix of \bar{v} . Now, in the group G we have

$1 = g_m = f_m = h_m = h$. Since h is a factor of \bar{v} and \bar{v} is G -reduced, we conclude that $h = 1$ as a word. This allows to conclude that $f_m = g_m = h_m = 1$ as words. Again, by left-right symmetry, we may assume that \bar{x}_m is a prefix of x_{m+1} . Thus, both in y_0 and in z_0 we replace the common factors $x_m \bar{x}_m$ by 1. Note that this has no influence on y or z . This yields a new assumption about x , y_0 , and z_0 , we have

$$x = x_1 f_1 \cdots x_{n'}$$

with $n' \leq n$ and a corresponding $m' = M' < m$. We repeat the procedure. There is only one way the procedure may stop. Namely at some point v is not an infinite factor anymore.

Hence, we are back at a situation of type:

$$y \xleftarrow[S_0]{*} y_1 \xleftarrow[S]{*} y_0 \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z.$$

This situation has already been solved.

Hence for the rest of this proof we may assume $m \neq M$. This is actually the most difficult part. By making f_m and f_M larger, we may assume that $g_m = h_m = 1$ as words. Note that for some letter a we have $x_m = x'a$ and $x_{m+1} = \bar{a}x''$. Assume that h_m is covered by $v\bar{v}$. Then $ah_m\bar{a}$ appears as a non-trivial factor in $v\bar{v}$, where $ah_m\bar{a} \xrightarrow[S_0]{*} 1$. Since both v and \bar{v} are G -reduced, we end up with $m = M$, which has been excluded. Thus, h_m is not covered by $v\bar{v}$. We conclude that we may assume $f_m = g_m = h_m = 1$ as words. By symmetry, g_M is not covered by $u\bar{u}$ and $f_M = g_M = h_M = 1$ as words. In particular we have $k \leq K$. More precisely, we are now faced with the following situation:

$$1 = \ell \leq m \leq L \leq k \leq M \leq K = n.$$

Without restriction we can therefore write:

$$\begin{aligned} x &= x_1 f_1 \cdots x_L f_L \cdots f_{k-1} x_k \cdots f_{n-1} x_n \\ y_0 &= x_1 g_1 \cdots x_{k-1} g_{k-1} x_k f_k x_{k+1} \cdots f_{n-1} x_n = u\bar{u}y \\ z_0 &= x_1 f_1 \cdots x_{L-1} f_{L-1} x_L h_L x_{L+1} \cdots h_{n-1} x_n = zv\bar{v} \\ y &= f_k x_{k+1} \cdots f_{n-1} x_n \\ z &= x_1 f_1 \cdots x_{L-1} f_{L-1} \end{aligned}$$

Consider the *overlapping* factor $\tilde{x} = x_L f_L \cdots f_{k-1} x_k$ inside the word x . Define new words $w_g = x_L g_L \cdots g_{k-1} x_k$ and $w_h = x_L h_L \cdots h_{k-1} x_k$. We claim that

there are G -reduced words U and V such that

$$\begin{aligned} y &\xRightarrow[S_0]{*} V\overline{V}w_h, \\ z &\xRightarrow[S_0]{*} \overline{w}_g U\overline{U}. \end{aligned}$$

By symmetry it is enough to show that $y \xRightarrow[S_0]{*} V\overline{V}w_h$. Consider

$$y_0 = x_1 g_1 \cdots x_{k-1} g_{k-1} x_k f_k x_{k+1} \cdots f_{n-1} x_n.$$

Since $f_M = 1$ we know that $x_L f_L x_{L+1} \cdots f_{M-1} x_M$ reduces to the word v and hence $x_{M+1} f_{M+1} \cdots f_{n-1} x_n$ reduces to \overline{v} . Moreover, we can write $v = w_h V$ with

$$f_k x_{k+1} \cdots f_{M-1} x_M \xRightarrow[S_0]{*} V.$$

As V appears in a factor of v it is G -reduced. We obtain the claim:

$$y = f_k x_{k+1} \cdots f_{M-1} x_M x_{M+1} f_{M+1} \cdots f_{n-1} x_n \xRightarrow[S_0]{*} V\overline{V}w_h.$$

Since S_0 is confluent and $w_g \xleftarrow[S_0]{*} \tilde{x} \xrightarrow[S_0]{*} w_h$, we find w such that

$$\overline{w}_h \xRightarrow[S_0]{*} w \xleftarrow[S_0]{*} \overline{w}_g$$

Hence:

$$y \xRightarrow[\text{Big}]{\leq 1} w \xleftarrow[\text{Big}]{\leq 1} z.$$

This shows that the system S in Equation 2 is confluent. This finishes the proof of the lemma and therefore of Theorem 5.3, too. \square

Corollary 5.5. *The canonical homomorphism $G \rightarrow E(A, G)$ is an embedding.*

Proof. Let $x, y \in \Gamma^*$ be finite words such that $x = y$ in $E(A, G)$. Then we have $x \xRightarrow[S]{*} w \xleftarrow[S]{*} y$ for some $w \in \Gamma^*$. But this implies $x \xRightarrow[S_0]{*} w \xleftarrow[S_0]{*} y$. Hence $x = y$ in G . \square

Corollary 5.6. *Let S_0 be a convergent system defining the group G . The canonical mapping*

$$\text{IRR}(S_0) \cap R(A, G) \rightarrow E(A, G)$$

is injective.

Proof. Since the system S is confluent (hence Church-Rosser), the canonical mapping $\text{IRR}(S) \rightarrow E(A, G)$ is injective. The result follows, because Lemma 5.2 tells us $\text{IRR}(S) \cap R(A, G) = \text{IRR}(S_0) \cap R(A, G)$. \square

The following special case is used in Section 6.

Corollary 5.7. *Let $G = F(\Sigma)$ be a free group. Then pairwise different freely reduced closed words are mapped to pairwise different elements in $E(A, G)$.*

Proof. For $G = F(\Sigma)$ we can choose S_0 to contain just the trivial rules $a\bar{a} \rightarrow 1$, where $a \in \Gamma = \Sigma \cup \Sigma^{-1}$. The system is convergent and

$$\text{IRR}(S_0) = R(A, G) = \{u \in W(A, G) \mid u \text{ is freely reduced}\}.$$

The result follows by Corollary 5.6. \square

Example 5.8. *Let $a \in \Sigma$ and $u, v \in F(\Sigma)$ be represented by non-empty cyclically reduced words in Γ^* . (For example u, v are themselves letters.) Consider the following infinite closed words:*

$$\begin{aligned} w &= [uuu \cdots](\cdots vvv) \\ z &= [uuu \cdots](\cdots aaa)[\bar{a}\bar{a}\bar{a} \cdots](\cdots \bar{v}\bar{v}\bar{v}) \end{aligned}$$

The word w is freely reduced (hence irreducible w.r.t. the system S_0 , but z is not freely reduced and S_0 is not terminating on z .

By Corollary 5.6 we have $uw = wv$ in $E(A, G)$ if and only if $uw = wv$ in $W(A, G) \mid u| = |v|$.

Although the word z has no well-defined length one can infer the same conclusion. First let $|u| = |v|$, then $z = uz\bar{v}$ in $E(A, G)$ and hence $uz = zv$. For the other direction write $z = z'\bar{v}$ as words and let $uz = zv = z'$ in $E(A, G)$. Then $uz \xrightarrow[S]{} \tilde{z} \xleftarrow[S]{*} z'$ for some word \tilde{z} .*

After cancellation of factors $a^m\bar{a}^m$ inside $(\cdots aaa) \cdot [\bar{a}\bar{a}\bar{a} \cdots]$ the borderline between a 's and \bar{a} 's must match inside \tilde{z} . So exactly $|u|$ more cancellations of type $a\bar{a} \rightarrow 1$ inside uz took place than in z' . Hence $|u| = |v|$. The other direction is trivial.

For each ordinal $d \in \Omega$ let

$$\mathcal{G}_d = \{x \in E(A, G) \mid x \text{ is given by some word of degree at most } d\}$$

Corollary 5.5 has an obvious generalization. The proof is by transfinite induction and left to the interested reader.

Corollary 5.9. *Let $d \leq e \in \Omega$. Then the canonical homomorphism $\mathcal{G}_d \rightarrow \mathcal{G}_e$ is an embedding.*

The group $E(A, G)$ is the union of all \mathcal{G}_d , but if G is finite nothing interesting happens, we have $G = E(A, G)$ in this case because there are no infinite G -reduced words. However if G is infinite, then $E(A, G)$ may become huge due to the following observation.

Proposition 5.10. *Let A have rank at least 2. Then the following assertions are equivalent:*

i.) *The group G is infinite.*

ii.) *For all $d < e \in \Omega$ we have $\mathcal{G}_d \neq \mathcal{G}_e$.*

Proof. We have $|\Omega| \geq 2$. Let $d < e \in \Omega$ with $\mathcal{G}_d = \mathcal{G}_e$. We show that G is finite. Assume the contrary, then by Lemma 3.1 there is some G -reduced word x of degree e . Assume we find a word z of degree at most d such that $x \xrightarrow[S]{*} z$. Then, by confluence of S we have $x \xrightarrow[S]{*} y \xleftarrow[S]{*} z$ for some y of degree at most d . But now Lemma 5.2 tells us that $x \xrightarrow[S_0]{*} y$, which implies that x is of degree d , too. This is a contradiction, because rules from S_0 cannot decrease any degree other than 0. \square

The notion of a pre-perfect system from Definition 2.4 can be applied to rewriting systems over $W(A, \Gamma)$, too. In this case Theorem 5.3 implies the following result.

Corollary 5.11. *If the group G is defined by some pre-perfect string rewriting system S_0 , then the system S on $W(A, \Gamma)$ is also pre-perfect.*

Definition 5.12. *A word $x \in W(A, \Gamma)$ is called a local geodesic, if it has no finite factor f such that $f = g$ in G and $|g| < |f|$.*

Proposition 5.13. *Let G be presented by some pre-perfect string rewriting system $S_0 \subseteq \Gamma^* \times \Gamma^*$. Let $x \in W(A, \Gamma)$ be a local geodesic. Then $x \xrightarrow[S]{*} y$ implies both $x \xrightarrow[S_0]{*} y$ and $|x| = |y|$.*

Proof. Straightforward from Lemma 5.2 since local geodesics are G -reduced. \square

6 Torsion elements in $E(A, G)$ and cyclic decompositions

This section can be skipped if the reader is interested in the Word Problem of $E(A, G)$, only. We consider an infinite group G and we assume that A is non-Archimedean, i.e., A has rank at least 2. We show that $E(A, G)$ is never torsion

free. More precisely, $E(A, G)$ has always elements of order 2. Actually, often these elements generate $E(A, G)$, see Proposition 6.1. Torsion elements which are not conjugated to torsion elements in G can be represented as infinite fixed points of the involution, i.e., by infinite closed words x satisfying $x = \bar{x}$, see Proposition 6.2. In particular, all "new" torsion elements have order 2.

According to Lemma 3.1 there exists a (non-closed) partial word $p : \mathbb{N} \rightarrow \Gamma$, which is G -reduced. This defines a closed word $[p](\bar{p})$ for each length $(m, 1)$. More formally, for $m \in \mathbb{Z}$ define

$$\begin{aligned} w_m : [(0, 0), (m, 1)] &\rightarrow \Gamma \\ (n, 0) &\mapsto \frac{p(n)}{p(m-n)} \quad \text{for } n \geq 0 \\ (n, 1) &\mapsto \frac{p(m-n)}{p(n)} \quad \text{for } n \leq m \end{aligned}$$

We have $\overline{w_m} = w_m$ and hence $w_m^2 = 1$ in $E(A, G)$. By Theorem 5.3 the element w_m is not trivial, hence w_m has order 2.

In order to make the reasoning more transparent, assume that $G = F(\Sigma)$ is free. Then for $a \in \Sigma$ we may consider closed words $w_m = [aaa \cdots](\cdots \bar{a}\bar{a}\bar{a}) \in W(A, F(\Sigma))$. These words are pairwise different and freely reduced. By Corollary 5.7 reading $w_m \in E((A, F(\Sigma)))$, these elements are still non-trivial, pairwise different, and of order 2.

We have seen that $E(A, G)$ contains infinitely many elements of order 2. Actually, frequently these elements generate $E(A, G)$.

Proposition 6.1. *Let $G = F(\Sigma)$ and $|\Sigma| \geq 2$. Assume that Ω is a limit ordinal, that is for each $d \in \Omega$, we have $d + 1 \in \Omega$, too. Then $E(A, G)$ is generated by elements of order 2.*

Proof. Let x be cyclically reduced with $\deg(x) = d$. (If x is freely reduced, but xx is not, then we can choose some $a \in \Sigma$ such that xa is cyclically reduced since $|\Sigma| \geq 2$.)

We are going to define a freely reduced word x_∞ of length t_{d+1} as follows. For $1 \leq \alpha < t_{d+1}$ we let $x_\infty(\alpha) = x^k(\alpha)$, where $k \in \mathbb{N}$ is large enough that $|x^k| \geq \alpha$. Moreover, we let $x_\infty(t_{d+1} - \alpha + 1) = \overline{x_\infty(\alpha)}$.

Clearly, x_∞ is freely reduced and $\overline{x_\infty} = x_\infty$, hence x_∞ is of order 2. Moreover, by construction, $xx_\infty = x_\infty \bar{x}$. Hence, xx_∞ has order 2, and $x = (xx_\infty)x_\infty$ is the product of two elements of order 2. Since a_∞ is defined for $a \in \Sigma$, we see that all freely reduced words are a product of at most 4 elements of order 2. Now, freely reduced words generate $E(A, F(\Sigma))$, therefore elements of order 2 generate this group. \square

Clearly, as $G \subseteq E(A, G)$, all torsion elements of G appear in $E(A, G)$ again, so we can conjugate them and have many more torsion elements.

Proposition 6.2. *Let $x \in E(A, G)$ be a torsion element which is not conjugated to any element in G . Then there is a reduction $x \xrightarrow[S]{*} y$ such that $y = \bar{y}$. In particular, we have $x^2 = 1 \in E(A, G)$.*

Proof. Choose $x \xrightarrow[S]{*} y$ such that $d \in \Omega$ is minimal and $|y| = n_d t_d + \ell$ with $\deg(\ell) < d$. Moreover, among these y let the leading coefficient $n_d \in \mathbb{N}$ be minimal, too. Note that y cannot contain any factor $uv\bar{u}$ where $\deg(v) < \deg(u) = d$ and $v \xrightarrow[S]{*} 1$. Since x has torsion, we may assume $x^k = 1 \in E(A, G)$ for some $k > 1$. Hence $y^k \xrightarrow[S]{*} 1$ due to confluence of S . Now, $\deg(y^k) = d$, hence $y^k \xrightarrow[S]{*} 1$ implies that y^k has a factor $uv\bar{u}$ where $\deg(v) < \deg(u) = d$ and $v \xrightarrow[S]{*} 1$. Making v larger and u (and \bar{u}) smaller, we can factorize $v = v_1 v_2$ such that uv_1 is a suffix of y and $v_2 \bar{u}$ is a prefix of y . Moreover, for some closed word z of degree d we have $uv_1 \xrightarrow[S]{*} z \xleftarrow[S]{*} u\bar{v}_2$. Hence we can assume that z is a suffix of y and \bar{z} is a prefix of y . If z and \bar{z} overlap in y (that is $|y| < 2|z|$), then we have $y = \bar{y}$. Otherwise we write $y = \bar{z}y'z$ and we replace x by y' and we use induction. \square

7 Group extensions over $A = \mathbb{Z}[t]$

For the remainder of the present paper we assume that $A = \mathbb{Z}[t]$. This means A is the additive group of the polynomial ring over \mathbb{Z} in one variable t . The reason for the choice of A is that we wish the subgroup $A^{\deg < d}$ to be finitely generated for each degree $d \in \Omega$ where:

$$A^{\deg < d} = \{\beta \in A \mid \deg(\beta) < d\}.$$

This assumption is clear for $A = \mathbb{Z}[t]$, because each such subgroup is isomorphic to \mathbb{Z}^d with $d \in \mathbb{N}$. Moreover, every finitely generated subgroup H of $E(A, G)$ sits inside some $E(\mathbb{Z}^d, G)$.

We shall use the following well-known fact:

Lemma 7.1. *Let $k \geq 0$ and*

$$A_0 \subseteq A_1 \subseteq A_2 \subseteq A_3 \cdots$$

be an infinite ascending chain of subgroups in \mathbb{Z}^k . Then this chain becomes stationary, i.e., there is some m such that $A_m = A_n$ for all $n \geq m$.

7.1 Proper periods

Let $w \in W(A, \Gamma)$ be a word of length $\alpha \in A$, given as a mapping $w : [1, \alpha] \rightarrow \Gamma$. An element $\pi \in A$ is called a *period* of w , if for all $\beta \in A$ such that $1 \leq \beta$, $\beta + \pi \leq \alpha$ we have

$$w(\beta) = w(\beta + \pi).$$

A period π is called a *proper period* of w , if $\deg(\pi) < \deg(w)$. In the following we are interested in proper periods, only. We have the following basic lemma.

Lemma 7.2. *Let $w \in W(A, \Gamma)$ of degree $\deg(w) = d$ with $0 \leq d$, then the set $\Pi(w)$ of proper periods forms a subgroup of $A^{\deg < d}$.*

Proof. We have $0 \in \Pi(w)$. If $\pi \in \Pi(w)$, then $-\pi \in \Pi(w)$, too. Let $\pi', \pi \in \Pi(w)$ with $0 \leq \pi' \leq \pi$. Clearly, $\pi + \pi'$ is a proper period, too. It remains to show that $\pi - \pi'$ is a proper period. To see this, let $\beta \in A$ such that $0 \leq \beta$, $\beta + \pi - \pi' \leq |w|$. For $\beta + \pi \leq |w|$ the element $\pi - \pi'$ is a proper period, because then $w(\beta) = w(\beta + \pi) = w(\beta + \pi - \pi')$. Hence we may assume that $\beta + \pi > |w|$. But $\deg(\pi) < \deg(w)$, hence $\deg(\beta) = \deg(w)$ and therefore $0 \leq \beta - \pi'$. Thus, $w(\beta) = w(\beta - \pi') = w(\beta + \pi - \pi')$. \square

Together with Lemma 7.1 the lemma above leads us to the following observation:

Proposition 7.3. *Let $w_0, w_1, w_2, w_3, \dots$ be an infinite sequence of elements of $W(A, \Gamma)$ such that w_{i+1} is always a non-empty factor of w_i . Let*

$$\Pi_0, \Pi_1, \Pi_2, \Pi_3, \dots$$

be the corresponding sequence of proper periods in A . Then this sequence of groups becomes stationary, i.e., there is some m such that $\Pi_m = \Pi_n$ for all $n \geq m$.

Proof. The sequence of degrees is descending and becomes stationary. Hence we may assume that in fact

$$0 \leq \deg(w_0) = \deg(w_1) = \deg(w_2) = \deg(w_3) = \dots$$

As a consequence

$$\Pi_0 \subseteq \Pi_1 \subseteq \Pi_2 \subseteq \Pi_3 \dots$$

is an ascending chain of subgroups in some \mathbb{Z}^k which becomes therefore stationary. \square

8 Deciding the Word Problem in $E(A, G)$

Recall that for a finitely generated group the decidability of the Word Problem does not depend on the presentation: It is a property of the group. In the following we restrict ourselves to the case that Γ is finite (in particular, G is finitely generated). The main difficulty for deciding the Word Problem in $E(A, G)$ is due to periodicity.

8.1 Computing reduced degrees

Let S be the system defined in Equation 2 which is confluent by Theorem 5.3. If we have $x \xrightarrow[S]{*} y$ then we have $\deg(x) \geq \deg(y)$. Thus, we can define the *reduced degree* by

$$\text{red-deg}(x) = \min \left\{ \deg(y) \mid x \xrightarrow[S]{*} y \right\}.$$

Note that $\text{red-deg}(x)$ is well-defined for group elements $x \in E(A, G)$ due the confluence of S .

Lemma 8.1. *Let $u \in R(A, G)$ be a non-empty G -reduced word. Then we have $0 \leq \deg(u) = \text{red-deg}(u)$.*

Proof. This is a direct consequence of Lemma 5.2. □

Clearly, since G is a subgroup of $E(A, G)$, the Word Problem of G must be decidable, otherwise we cannot hope to decide the Word Problem for finitely generated subgroups of $E(A, G)$.

Our goal is to solve the Word Problem in $E(A, G)$ via the following strategy. We compute on input $w \in W(A, \Gamma)$ some $w' \in W(A, \Gamma)$ such that both $w \xrightarrow[S]{*} w'$ and $\deg(w') = \text{red-deg}(w)$. If $\deg(w') > 0$, then $w \neq 1$ in $E(A, G)$. Otherwise w' is a finite word over Γ and we can use the algorithm for G which decides whether or not $w' = 1$ in $G \subseteq E(A, G)$.

In order to achieve this goal we need a slightly stronger condition on G . We need that the non-uniform cyclic membership problem in G is decidable. This means that for each $v \in \Gamma^*$ there is an algorithm $\mathcal{A}(v)$ which solves the problem " $u \in \langle v \rangle$?". Thus, $\mathcal{A}(v)$ decides on input $u \in \Gamma^*$ whether or not u (as an element of G) is in the subgroup of G which is generated by v . This requirement on G is indeed a necessary condition:

Theorem 8.2. *Assume that the Word Problem is decidable for each finitely generated subgroup of $E(A, G)$. Then for each $v \in \Gamma^*$ there exists an algorithm which decides on input $u \in \Gamma^*$ whether or not u (as an element of G) is in the subgroup of G which is generated by v .*

Proof. Let $v \in \Gamma^*$ be a finite word. If v is empty we are done because " $u \in \langle 1 \rangle$?" is nothing but the Word Problem for G (which is a finitely generated subgroup of $E(A, G)$). Hence we may assume that v is non-empty and moreover, $v \neq 1$ in G . If v is a torsion element, then the question whether or not u is in the subgroup generated by v can be reduced to the Word Problem. Hence may assume that $v^k \neq 1$ for all $k \neq 0$. We perform an induction on the length of v which allows to view v as a finite G -reduced word.

We can solve the problem " $u \in \langle v \rangle$?" for all inputs u as soon as we can solve the problem " $u \in \langle pv^k\bar{p} \rangle$?" for some p and $k \neq 0$ for all inputs u . Indeed, fix p and k . Then, $u \in \langle v \rangle$ if and only if $puv^i\bar{p} \in \langle pv^k\bar{p} \rangle$ for some $0 \leq i < |k|$. Clearly, $puv^i\bar{p} \in \langle pv^k\bar{p} \rangle$ implies $u \in \langle v \rangle$. For the other direction let $u = v^m$. We can write $m = \ell k - i$ with $\ell \in \mathbb{Z}$ and $0 \leq i < |k|$. It follows $puv^i\bar{p} \in \langle pv^k\bar{p} \rangle$. Thus, the problem " $u \in \langle v \rangle$?" is reduced to the problem:

$$"\exists i : 0 \leq i < |k| \quad \& \quad puv^i\bar{p} \in \langle pv^k\bar{p} \rangle?"$$

Therefore, by induction on $|v|$ we may assume that no proper factor w of the word v is equal to any $pv^k\bar{p}$ in G . (We only need the existence of an algorithm. There is no need to construct the algorithm on input v .)

Next, we claim that every power v^m is G -reduced. Assume the contrary, then there are words p, q, r, s and $k \in \mathbb{N}$ such that $v = pq = rs$ and $q \neq v \neq r$ as words, but $qv^k r = 1$ in G . Note that neither r nor q can be the empty word by the induction hypothesis. Moreover, $p \neq r$ because $v^{k+1} \neq 1$ in G . If $|p| < |r|$, then we can write $r = pw$ where w is a proper factor of v , and we obtain

$$1 = qv^k pw = \bar{p}pqv^k pw = \bar{p}v^{k+1}pw.$$

This is impossible since no proper factor of v is of the form $pv^{-k-1}\bar{p}$ in G .

If $|p| > |r|$, then $p = rw$ for some proper factor w of v . We obtain $qv^k p = w$ in G . Again this is impossible, because it would imply $qv^k pq\bar{q} = qv^{k+1}\bar{q} = w$ in G .

Thus, $V = [vvv \dots](\dots vvv)$ is a G -reduced word of degree 1 in $E(A, G)$. Next, we may assume that v is a primitive word, this means v is no proper power of any other word. It follows that v does not appear properly inside vv as a factor.

We claim that now, $u \in \langle v \rangle$ if and only if $uV = Vu$ in $E(A, G)$. Clearly, if $u \in \langle v \rangle$ then $uV = Vu$ in $E(A, G)$. For the other direction let $uV = Vu$ in $E(A, G)$. Then by applying finitely many times defining relations for G we must be able to transform the one-sided partial infinite word $uvvv\dots$ into $vvv\dots$. Thus for some word $w \in \Gamma^*$, a factorization $v = pq$, and $k, \ell \in \mathbb{N}$ we obtain $wv^k = v^\ell p$ in G such that the infinite words $wvvv\dots$ and $wqv^k v\dots$ are equal. But v is primitive and hence $p \in \{1, v\}$. Thus, $u \in \langle v \rangle$. \square

Theorem 8.3. *Let G be a group such that for each $v \in \Gamma^*$ there is an algorithm which decides on input $u \in \Gamma^*$ whether or not $u \in G$ is in the subgroup of G generated by v .*

Then for each finite subset $\Delta \subseteq W(A, \Gamma)$ of G -reduced words (i.e., $\Delta \subseteq R(A, G)$) there is an algorithm which computes on input $w \in \Delta^$ its reduced degree and some $w' \in W(A, \Gamma)$ such that both $w \xrightarrow[S]{*} w'$ and $\deg(w') = \text{red-deg}(w)$.*

Proof. The proof is split into two parts. The first part is a preprocessing on the finite set Δ . In the second part we present the algorithm for the set Δ after the preprocessing.

PART I: Preprocessing

The preprocessing concerns Δ and not the actual algorithm. Therefore it is not an issue that the steps in the preprocessing are effective. It is clear that we may replace Δ by any other finite set $\hat{\Delta}$ such that $\Delta \subseteq \hat{\Delta}^*$. This is what we do. We apply the following transformation rules in any order as long as possible, and we stop if no rule changes Δ anymore. The result is $\hat{\Delta}$ which is, as we will see, still a set of G -reduced words. (This will follow from the fact that every factor of a G -reduced word is G -reduced).

- 1.) Replace Δ by $(\Delta \cup \Gamma) \setminus \{1\}$. (Recall that Γ is finite in this section.)
- 2.) If we have $g \in \Delta$, but $\bar{g} \notin \Delta$, then insert \bar{g} to Δ .
- 3.) If we have $g \in \Delta$ with $g = fh$ in $W(A, \Gamma)$ and $\deg(g) = \deg(f) = \deg(h)$, then remove g and \bar{g} from Δ and insert f and h to Δ .

After these steps every element in Δ has its inverse in Δ and for some $d \in \mathbb{N}$ it has a length of the form $t^d + \ell$ with $\deg(\ell) < d$. Thus, the leading coefficient is always 1. In particular, all generators of finite length are letters of $\Gamma = \Sigma \cup \bar{\Sigma}$. The next rules are more involved. We first define an equivalence relation on $W(A, \Gamma)$. We let $g \sim h$ if for some x, y, z, t , and u in $W(A, \Gamma)$ with $\deg(xyzt) < \deg(u)$ we have

$$g = xuy \quad \text{and} \quad h = zut.$$

Note that the condition implies $\deg(g) = \deg(u) = \deg(h)$. The effect of the next rule is that for each equivalence class there is at most one group generator in Δ .

- 4.) If we have $g, h \in \Delta$ with $g \notin \{h, \bar{h}\}$, but $g = xuy$ and $h = zut$ for some x, y, z, t , and u with $\deg(xyzt) < \deg(u)$, then remove g, h, \bar{g}, \bar{h} from Δ and insert x, y, z, t (those which are non-empty) and u to Δ .

- 5.) If we have $g \in \Delta$ with $g \neq \bar{g}$, but $g = xuy = z\bar{u}t$ for some x, y, z, t , and u with $\deg(xyzt) < \deg(u)$, then write $u = pq$ with $\deg(p) < \deg(q) = \deg(u)$ and $q = \bar{q}$. Remove g and \bar{g} from Δ and insert x, y, z, t, p, \bar{p} (those which are non-empty) and q to Δ . (Note that $g \sim q$.)

The next rules deal with periods.

- 6.) If we have $g \in \Delta$ and $g = xuy$ for some x, y , and u with $\deg(xy) < \deg(u)$ such that u has a proper period which is not a period of g , then remove g, \bar{g} from Δ and insert x, y (those which are non-empty) and u to Δ .

The following final rule below makes Δ larger again, and the rule adds additional information to each generator. For each $g \in \Delta$ let $\Pi(g) \subseteq A$ the group of proper periods. Let $B(g)$ be a set of generators of $\Pi(g)$. We may assume that for each possible degree d there is at most one element $\beta \in B(g)$ of degree d . Moreover, we may assume $0 \leq \beta$ and for each g the set $B(g)$ is fixed. In particular, for $\pi \in \Pi(g)$ with $\deg(\pi) = d \geq 0$ there is exactly one $\beta \in B(g)$ such that $\deg(\beta) = d$ and $\pi = m\beta + \ell$ for some unique $m \in \mathbb{Z}$ and $\ell \in \Pi(g)$ with $\deg(\ell) < d$. For each $\beta \in B(g)$ let $r(\beta)$ be the prefix and $s(\beta)$ be the suffix of length β of g . (In particular, $r(\beta)g = gs(\beta)$ in $W(A, \Gamma)$.) Note that the number of $r(\beta), s(\beta)$ is bounded by $2 \deg(g)$.

- 7.) If we have $g \in \Delta$, then let $B(g)$ be a set of generators for the set of proper periods $\Pi(g)$ as above. If necessary, enlarge Δ by finitely many elements of degree less than $\deg(g)$ (and which are factors of elements of Δ) such that $r(\beta), s(\beta) \in \Delta^*$ for all $\beta \in B(g)$.

Note that the rules 1.) to 7.) can be applied only a finite number of times. The formal proof relies on König's Lemma and Proposition 7.3.

Remark 8.4. *Note that the preprocessing has been done in such a way that every element in $\hat{\Delta}$ is either a letter or a factor of an element in the original set Δ . In particular, if Δ contains local geodesics only, then $\hat{\Delta}$ has the same property. This fact is used for Corollary 8.6.*

PART II: An algorithm to compute the reduced degree

We may assume that Δ has passed the preprocessing, i.e., $\Delta = \hat{\Delta}$ and no rule above changes Δ anymore. The input w (to the algorithm we are looking for) is given as a word $g_1 \cdots g_n$ with $g_i \in \Delta$. Let

$$d = \max \{ \deg(g_i) \mid 1 \leq i \leq n \}.$$

We may assume that $d > 0$. Either $\deg(w) = \text{red-deg}(w)$ (and we are done) or $\deg(w) > \text{red-deg}(w)$ and $w \in W(A, \Gamma)$ contains a factor $uv\bar{u}$ such that the following conditions hold:

- 1.) The word u is G -reduced and has length $|u| = t^d + \ell$ with $\deg(\ell) < d$,
- 2.) $\deg(v) < d$,
- 3.) $v \xrightarrow[S]{*} 1$.

We may assume that the factor $uv\bar{u}$ starts in some g_i and ends in some g_j with $i < j$, because the leading coefficient of each length $|g_i| \in \mathbb{Z}[t]$ is 1. Moreover, by making u smaller and thereby v larger, we may in fact assume that u is a factor of g_i and \bar{u} is a factor of g_j . Thus, $\deg(g_i) = \deg(u) = \deg(g_j) = d$ and we can write $g_i = xuy$ and $g_j = z\bar{u}t$. By preprocessing on Δ (Rule 4), we must have $g_i \in \{g_j, \bar{g}_j\}$. Assume $g_i = g_j$, then we have $g_i = xuy = z\bar{u}t$ and, by preprocessing on Δ (Rule 5), we may conclude $g_i = \bar{g}_i$. Thus in any case we know $g_i = \bar{g}_j$.

Thus, henceforth we can assume that for some $1 \leq i < j \leq n$ we have in addition to the above:

- 4.) $g_i = xuy$,
- 5.) $v = yg_{i+1} \cdots g_{j-1}z$,
- 6.) $g_j = z\bar{u}t = \bar{g}_i$.

Since $g_j = z\bar{u}t = \bar{g}_i$ we have $xuy = \bar{t}u\bar{z}$, and by symmetry (in i and j) we may assume:

- 7.) $|y| \geq |z|$.

This implies $y = q\bar{z}$ for some $q \in W(A, \Gamma)$ with $\deg(q) < d$ and $uq = q'u$ for $\bar{t} = xq'$.

Therefore $|q|$ is a proper period of u , and hence, by preprocessing on Δ (Rule 6), we see that $|q|$ is a proper period of g_i . Thus there are $p', p \in \Delta^*$ with $|p'| = |p| = |q|$ such that $p'g_i = g_ip$. But \bar{z} and y are suffixes of g_i , hence

$$y = \bar{z}p.$$

Therefore:

- 8.) $pg_{i+1} \cdots g_{j-1} \xrightarrow[S]{*} 1$, where p is a suffix of g_i and $|p|$ is a proper period of g_i .

We know $\deg(g_{i+1} \cdots g_{j-1}) < d$. Hence by induction on d we can compute $h \in \Delta^*$ such that both $g_{i+1} \cdots g_{j-1} \xleftarrow[S]{*} h$ and $\deg(h) = \text{red-deg}(g_{i+1} \cdots g_{j-1})$. This implies $\deg(h) = \text{red-deg}(p)$, too. But p is a factor of a G -reduced word, hence actually $\deg(h) = \deg(p)$ by Lemma 8.1.

We distinguish two cases. Assume first that $\deg(h) \leq 0$. Then $h, p \in \Gamma^*$ are finite words. If $h = 1$ in G , then we can replace the input word w by

$$g_1 \cdots g_{i-1} g_{j+1} \cdots g_n$$

since $g_i g_{i+1} \cdots g_{j-1} \bar{g}_i \xrightarrow[S]{*} 1$, and we are done by induction on n .

If $h \in \Gamma^*$ is a finite word, but $h \neq 1$ in G , then $p = h^{-1} \neq 1$ in G , too. Consider the smallest element $\rho \in B(g_i)$ and let $r \in \Gamma^*$ be the suffix of g_i with $|r| = \rho$. It follows that p is a positive power of r because $|p|$ is a period of g_i . This means that h is in the subgroup of G generated by r . For this test we have an algorithm by our hypothesis on G . According to our assumptions the answer of the algorithm is yes: h is in the subgroup generated by r . This allows to find $m \in \mathbb{Z}$ with $\bar{h} = r^m$ in the group G . We find some finite word s of length $|s| = |r^m|$ such that $sg_i = g_i r^m$; and we can replace the input word w by $g_1 \cdots g_{i-1} \bar{s} g_{j+1} \cdots g_n$, because we have:

$$\begin{aligned} g_1 \cdots g_i \cdots g_j \cdots g_n &\xleftrightarrow[S]{*} g_1 \cdots \bar{s} s g_i \cdots g_j \cdots g_n \\ &\xleftrightarrow[S]{*} g_1 \cdots \bar{s} g_i r^m h \bar{g}_i g_{j+1} \cdots g_n \\ &\xrightarrow[S]{*} g_1 \cdots \bar{s} g_i \bar{g}_i g_{j+1} \cdots g_n \\ &\xrightarrow[S]{} g_1 \cdots g_{i-1} \bar{s} g_{j+1} \cdots g_n. \end{aligned}$$

We are done by induction on the number of generators of degree d .

The final case is $\deg(h) > 0$. We write $|h| = m't^e + \ell$ with $\deg(\ell) < e = \deg(h)$. According to our preprocessing on Δ (Rule 7) there are words $r, s \in \Delta^*$ such that $\deg(r) = \deg(p)$, r is a suffix of g_i with $sg_i = g_i r$. For some m with $m \leq m'$ we must have $\text{red-deg}(r^m h) < e$. By induction we can compute some word f with $\deg(f) = \text{red-deg}(r^m h)$ and $f \xleftrightarrow[S]{*} r^m h$. Like above we can replace the input word w by

$$g_1 \cdots g_{i-1} \bar{s}^m g_i f g_j \cdots g_n,$$

because we have:

$$\begin{aligned} g_1 \cdots \bar{s}^m s^m g_i \cdots g_j \cdots g_n &\xleftrightarrow[S]{*} g_1 \cdots \bar{s}^m g_i r^m h \bar{g}_i g_{j+1} \cdots g_n \\ &\xleftrightarrow[S]{*} g_1 \cdots \bar{s}^m g_i f \bar{g}_i g_{j+1} \cdots g_n. \end{aligned}$$

We are done by induction on the degree e which is the reduced degree of the factor $r^m g_{i+1} \cdots g_{j-1}$. We can apply this induction since $g_i r^m g_{i+1} \cdots g_{j-1} g_j$ now has a factor $uv\bar{u}$ such that the following conditions hold:

- 1.) The word u is G -reduced and $\deg(u) = d > 0$,

$$2.) \deg(v) < e,$$

$$3.) v \xrightarrow[S]{*} 1.$$

□

By Theorems 8.2 and 8.3 we obtain the following corollary which gives the precise answer in terms of the group G whether or not the Word Problem in finitely generated subgroups of $E(A, G)$ is decidable.

Corollary 8.5. *Let G be finitely generated by Γ and $A = \mathbb{Z}[t]$. Then the following assertions are equivalent:*

- i.) *For each $v \in \Gamma^*$ there is an algorithm which decides on input $u \in \Gamma^*$ the Cyclic Membership Problem " $u \in \langle v \rangle$?"*
- ii.) *For each finite subset $\Delta \subseteq W(A, \Gamma)$ there is an algorithm which decides on input $w \in \Delta^*$ whether or not $w = 1$ in the group $E(A, G)$.*

Recall that (according to Definition 5.12) a local geodesic denotes word without any finite factor f such that $f = g$ in G but $|g| < |f|$. Inspecting the proof above we find the following variant of Corollary 8.5.

Corollary 8.6. *Let G be finitely generated by Γ and $A = \mathbb{Z}[t]$. Then the following assertions are equivalent:*

- i.) *The group G has a decidable Word Problem.*
- ii.) *For each finite subset $\Delta \subseteq W(A, \Gamma)$ of local geodesics there is an algorithm which decides on input $w \in \Delta^*$ whether or not $w = 1$ in the group $E(A, G)$.*

Remark 8.7. *Clearly, Condition i.) in Corollary 8.5 implies Condition i.) in Corollary 8.6, but the converse fails. There is a finitely presented group G with a decidable Word Problem, but one can construct a specific word v such that the Cyclic Membership Problem " $u \in \langle v \rangle$?" is undecidable, see [24, 25].*

Remark 8.8. *Let G be a finitely generated group. Of course, if G has a decidable Generalized Word Problem, i.e., the Membership Problem w.r.t. finitely generated subgroups is decidable, then the Cyclic Membership Problem " $u \in \langle v \rangle$?" is decidable, too. Examples of groups G where the Generalized Word Problem is decidable include metabelian, nilpotent or, more general, abelian by nilpotent groups, see [27]. However, there are also large classes of groups, where the Membership Problem is undecidable, but the Cyclic Membership Problem is easy. For example, the Cyclic Membership Problem is decidable in linear time in a direct*

product of free groups, but as soon as G contains a direct product of free groups of rank 2, the Generalized Word Problem becomes undecidable by [20]. For hyperbolic groups a construction of Rips shows that the Generalized Word Problem is undecidable ([26]), but the Cyclic Membership Problem " $u \in \langle v \rangle$?" is decidable by [19].

Decidability of the the Cyclic Membership Problem is also preserved e.g. by effective HNN extensions. This means, if H is an HNN-extension of G by a stable letter t such that we can effectively compute Britton reduced forms, then one can reduce the Cyclic Membership Problem " $u \in \langle v \rangle$?" in H to the same problem in G as follows. On input u, v we compute first the Britton reduced form of v . This tells us whether $v \in G$. If so, we are done by checking first that $u \in G$ and then by using the algorithm for G . So, let $v \in H \setminus G$. Via conjugation we may assume that v^k remains Britton reduced for all $k \in \mathbb{Z}$. Now, if u is Britton reduced, too, then it is enough to check $u = v^k$ for that k where the t -sequence of u coincides with the one of v^k . There is at most one such k . Thus we can use the algorithm to decide the Word Problem in H which exists because we can effectively compute Britton reduced forms.

As every one-relator group G sits inside an effective HNN extension of another one-relator group with a shorter relator [18], we see that the Cyclic Membership Problem is decidable in one-relator groups, too. The property is also preserved by effective amalgamated products for a similar reason as for HNN extensions.

9 Realization of some HNN-extensions

The purpose of this section is to show that the group $E(A, G)$ contains some important HNN-extensions of G which therefore can be studied within the framework of infinite words. Moreover, we show that $E(A, G)$ realizes more HNN-extensions than it is possible in the approach of [22]. The reason is that [22] is working with cyclically reduced decompositions, only. We begin with this concept and we show first how it embeds in our setting.

9.1 Cyclically reduced decompositions over free groups

In [22] the partial monoid $\text{CDR}(A, \Sigma)$ has been defined for a free group $F(\Sigma)$.

As a set $\text{CDR}(A, \Sigma)$ consists of those freely reduced words x in $W(A, \Gamma)$ which admit a *cyclically reduced decomposition* $x = cu\bar{c}$ where u is cyclically reduced. If the decomposition exists, it is unique. Note that $c = [aaa \cdots](\cdots \bar{a}\bar{a}\bar{a})$ is freely reduced, but it is not in $\text{CDR}(A, \Sigma)$. On the other hand, for $a \neq b \in \Sigma$ we have

$$x = [aaa \cdots](\cdots \bar{a}\bar{a}\bar{a}baaa \cdots)(\cdots \bar{a}\bar{a}\bar{a}) \in \text{CDR}(A, \Sigma)$$

since $x = cb\bar{c}$.

In $\text{CDR}(A, \Sigma)$ a partial multiplication $x * y$ has been defined as follows. The result $x * y$ is defined if and only if $x = pq$, $y = \bar{q}r$, and pr is freely reduced. In this case $x * y = pr$. One can verify that $x * y$ admits a cyclically reduced decomposition.

In terms of our group $E(A, F(\Sigma))$ we can rephrase this as follows. The set $\text{CDR}(A, \Sigma)$ embeds into $E(A, F(\Sigma))$ because all elements are freely reduced and hence irreducible by the confluent system S . Now, $\text{CDR}(A, \Sigma)$ (being a subset of a group) becomes a partial monoid by defining $x * y$ as xy , in case $xy \in \text{CDR}(A, \Sigma)$. If $xy \notin \text{CDR}(A, \Sigma)$, then the result $x * y$ remains undefined. Clearly, if $x = pq$, $y = \bar{q}r$, and pr is freely reduced, then $x * y = pr = xy \in \text{CDR}(A, \Sigma) \subseteq E(A, F(\Sigma))$. Now, assume x, y , and $xy \in \text{CDR}(A, \Sigma)$. Then there exists a freely reduced word $z = cw\bar{c}$ where w is cyclically reduced such that $xy \xrightarrow[S]{*} z$. The reduction provides us with a factorization such that $x = pq$, $y = \bar{q}r$, and pr is freely reduced. Thus, $x * y$ is defined.

Let $a, b \in \Sigma$ with $a \neq b$. It is known that the HNN-extension of G by $sbs^{-1} = a$ with stable letter s embeds into $\text{CDR}(A, \Sigma)$ by letting $s = [aaa \cdots](\cdots bbb)$. To see this, observe that this HNN-extension can be written as a semi-direct product $F(a, b) \rtimes \mathbb{Z}$. This allows to write elements in normal form as a word $x = w \cdot s^k$ where w is a freely reduced word over Σ^\pm and $k \in \mathbb{Z}$. A direct inspection shows that x is in $\text{CDR}(A, \Sigma)$ and it is trivial in $E(A, F(\Sigma))$ if and only if it is trivial in $F(a, b) \rtimes \mathbb{Z}$.

However, the HNN-extension H of G by $sb^2s^{-1} = a^2$ does not embed into $\text{CDR}(A, \Sigma)$ because the commutation relation \sim is not transitive, but it is known to be transitive in any finitely generated subgroup of $\text{CDR}(A, \Sigma)$, [2]. The commutation relation is not transitive in H , because $a \sim a^2 = sb^2s^{-1} \sim sbs^{-1}$, but $a \not\sim sbs^{-1}$ in H .

The group $E(A, F(\Sigma))$ is however large enough to realize the HNN extension H , but we have to leave $\text{CDR}(A, \Sigma)$: Define

$$s = [aaa \cdots](\cdots ababab \cdots)(\cdots bbb).$$

Then the canonical homomorphism $H \rightarrow E(A, F(\Sigma))$ is an embedding. (See Proposition 9.4.) Note that $sb^2s^{-1} = a^2$, but $sbs^{-1} \neq a$ due to the middle line of ab 's which requires a shift by 2 in order to be matched. Clearly, $s, b, \bar{s} \in \text{CDR}(A, \Sigma)$ and $s' = s * b \in \text{CDR}(A, \Sigma)$ is defined. But $s' * \bar{s}$ is not defined, and therefore $sbs^{-1} \in E(A, F(\Sigma)) \setminus \text{CDR}(A, \Sigma)$. (Note that $s \cdot b \cdot s^{-1}$ is not a cyclically reduced decomposition, because $sb\bar{s}$ is not freely reduced and there is no freely reduced word x such that $x = sbs^{-1} \in E(A, F(\Sigma))$.) The element $s'\bar{s} = sb\bar{s}$ can be depicted as follows:

$$sb\bar{s} = [aaa \cdots](\cdots ababab \cdots)(\cdots bbb)[\bar{b}\bar{b} \cdots](\cdots bababa \cdots)(\cdots bb)b.$$

Remark 9.1. Let H be a subgroup inside the partial monoid $\text{CDR}(A, \Sigma)$, then H is torsion-free. Indeed $(cu\bar{c})^2 = cu^2\bar{c}$ and we can use Proposition 6.2. Since sbs^{-1} is torsion-free and $sbs^{-1} \in E(A, F(\Sigma)) \setminus \text{CDR}(A, \Sigma)$ for s and b as above, we see that the set of torsion elements is a proper subset of $E(A, F(\Sigma)) \setminus \text{CDR}(A, \Sigma)$, in general.

We conclude this subsection with a few more examples which allow similar calculations as above. In these examples we use however stable letters which have no cyclically reduced decomposition.

Example 9.2. Consider the following non-abelian semi-direct products: $G_1 = \mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})$ (which is isomorphic to the free product $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$) and $G_2 = \mathbb{Z} \rtimes \mathbb{Z}$. (which is isomorphic to the Baumslag-Solitar group $\text{BS}(1, -1)$.) The groups G_1 and G_2 can be embedded into $E(\mathbb{Z} \times \mathbb{Z}, \mathbb{Z})$. Indeed, define s_1 and s_2 as follows:

$$\begin{aligned} s_1 &= [aaa \cdots)(\cdots \bar{a}\bar{a}\bar{a}], \\ s_2 &= [aaa \cdots)(\cdots aaaa \cdots)(\cdots \bar{a}\bar{a}\bar{a}]. \end{aligned}$$

The element s_1 has order 2 and s_2 has infinite order in $E(\mathbb{Z} \times \mathbb{Z}, \mathbb{Z})$. Clearly $as_i = s_i\bar{a}$, and it is easy to verify that the subgroups generated by a and s_i are isomorphic to G_i for $i = 1, 2$.

Let $\Sigma \geq 2$ and let G_3 be the HNN-extension of \mathbb{Z} with stable letter s and defining relation $s^{-1}a^2s = a^{-2}$. The group G_3 is also the Baumslag-Solitar group $\text{BS}(2, -2)$. It embeds into $E(\mathbb{Z} \times \mathbb{Z}, F(\Sigma))$ using s_3 as a stable letter, where

$$s_3 = [aaa \cdots)(\cdots ababab \cdots)(\cdots \bar{a}\bar{a}\bar{a}].$$

Again, a direct verification that this group embeds is not difficult. All three embeddings occur as special cases of Proposition 9.4. None of these groups can be embedded into the partial monoid $\text{CDR}(A, \Sigma)$: The group G_1 is not torsion free and the commutation relation is not transitive neither in G_2 nor in G_3 .

9.2 Some HNN-extensions in $E(A, G)$

We continue with the assumption that $A = \mathbb{Z}[t]$. In [22] a power x^t with length $|x| \cdot t$ is constructed for $x \in \text{CDR}(A, \Sigma)$. (The partial monoid $\text{CDR}(A, \Sigma)$ has been defined in Section 9.1.) The construction of x^t fails however to satisfy $\bar{x}^t = \overline{x^t}$, in general. Thus, x^t cannot be used to define an HNN extension with stable letter x^t . We content ourselves to prove the following fact.

Proposition 9.3. *Let $x \in W(A, G)$ be a non-empty cyclically G -reduced word. Then we can define a free abelian subgroup X of $E(A, G)$ with countable basis $\{x_d \mid d \in \mathbb{N}\}$ such that $x_0 = x$. Hence, the homomorphism*

$$a_0 + a_1t + \cdots + a_nt^n \mapsto x^{a_0}(x_1)^{a_1} \cdots (x_n)^{a_n}$$

embeds the abelian group A into $E(A, G)$.

Proof. Let $\deg(x) = e \geq 0$ and $|x| = \alpha$.

For $k \in \mathbb{N}$ consider x^{2k} as a mapping $x^{2k} : [-k\alpha + 1, k\alpha] \rightarrow \Gamma$. We can extend this to a partial (non-closed) word $x^{\mathbb{Z}} : D \rightarrow \Gamma$, where the domain is $D = \{\delta \in \mathbb{Z}[t] \mid \deg(\delta) \leq e\}$. Note that $\bar{x}^{\mathbb{Z}}(\delta) = x^{\mathbb{Z}}(-\delta + 1)^{-1}$ for $\delta \in D$.

We define $x_A : A \rightarrow \Gamma$ as follows: We let $x_A(\beta) = x^{\mathbb{Z}}(\beta)$ for $\deg(\beta) \leq e$. For $\deg(\beta) > e$ write $\beta = t^{e+1}\gamma + \delta$ with $\delta \in D$; and let $x_A(\beta) = x^{\mathbb{Z}}(\delta)$.

Finally, let $x_0 = x$ and for every $d \geq 1$ let x_d be the restriction of x_A to the closed interval $[1, t^{e+d}]$.

The word x_d has length t^{e+d} and $|x|$ is a proper period. We have to show that $\bar{x}_d = (\bar{x})_d$ for $d \geq 1$. To see this, consider $1 \leq \beta \leq t^{e+d}$ and write $\beta = t^{e+1}\gamma + \delta$ with $\delta \in D$. Then:

$$\begin{aligned} \bar{x}_d(\beta) &= x_d(t^{e+d} - t^{e+1}\gamma - \delta + 1)^{-1} \\ &= x^{\mathbb{Z}}(-\delta + 1)^{-1} \\ &= \bar{x}^{\mathbb{Z}}(\delta) \\ &= (\bar{x})_d(\beta) \end{aligned}$$

Thus, $a_0 + a_1t + \cdots + a_nt^n \mapsto x^{a_0}(x_1)^{a_1} \cdots (x_n)^{a_n}$ is a homomorphism of abelian groups.

Assume $f(t) = a_0 + a_1t + \cdots + a_nt^n \mapsto 1 \in E(A, G)$, then $a_n = 0$ due to the degrees and the fact that x is a cyclically G -reduced word. By induction $f(t) = 0$. \square

We say that a non-empty word $w \in W(A, G)$ is *primitive* if w does not appear as a factor of ww other than as its prefix or as its suffix and if in addition \bar{w} is not a factor of ww . In particular, a primitive word does not have any non-trivial proper period. If on the other hand, we can write $ww = pwq$ with $1 \leq |p| < |w|$, then $|p|$ is a non-trivial period of w . Note that the word w which looks like $[ababab \cdots](\cdots ababab)$ has period 2, it is not primitive, but it is no power of any other element. Hence, unlike to the case of finite words, being primitive is a stronger condition than not being a power of any other element.¹

¹A power is an element u^k for $k \in \mathbb{Z}$ since we have not defined u^α for $\deg(\alpha) > 0$. However even in a more general context the assertions remain true: assume w and w' look like $[ababab \cdots](\cdots ababab)$ with $w = (ab)^\alpha$ and $w' = (ab)^\beta$, where $|w| = t$ and $|w'| = t + 1$. Then we should expect that $(ab)^{\beta-\alpha}$ is a power of ab , but this is not compatible with $|(ab)^{\beta-\alpha}| = 1$.

Note also that $ww = p\bar{w}q$ means that we can write $w = pq$ with $\bar{p} = p$ and $\bar{q} = q$. It follows that w is primitive if and only if \bar{w} is primitive. For a non-abelian free group $F(\Sigma)$ primitive cyclically reduced words of every positive length exist: Consider w with $w(1) = a$ and $w(\beta) = b$ otherwise.

Let H be a subgroup of $E(A, G)$ and $u \in H$ be a cyclically G -reduced element. As usual the *centralizer* of u in H is the subgroup $\{v \in H \mid uv = vu\}$.

Proposition 9.4. *Let H be a finitely generated subgroup of $E(A, G)$ and let $u, v, w \in H$ be (not necessarily different) cyclically G -reduced elements such that $|u| = |v| = |w|$ and such that w is primitive. In addition, let u and v have cyclic centralizers in H . Then the HNN extension*

$$H' = \langle H, t \mid s^{-1}us = v \rangle$$

embeds into $E(A, G)$.

Proof. Let $\deg(u) = e$. We have $e \geq 0$. Since H is finitely generated, there is a degree d (with $d > e$) such that $\deg(x) < d$ for all $x \in H$. By the construction according to Proposition 9.3 we define the following elements $U = u_{d-e-1}$, $V = v_{d-e-1}$, and $W = w_{d-e-1} \in E(A, G)$. Recall that $|U| = |V| = |W| = |w|$ for $d = e + 1$ or $|U| = |V| = |W| = t^{d-1}$ for $d > e + 1$. The abelian group of proper periods $\Pi(W)$ is trivial or it is generated by $|w|$ and t^{e+1}, \dots, t^{d-2} . The groups $\Pi(U)$ and $\Pi(V)$ may have larger rank than $d - e$.

Let us define a word s of length $2t^d$ which is depicted as follows:

$$s = [UUU \dots](\dots WW \dots)(\dots VVV).$$

The group $\Pi(s)$ is generated by $|w|$ and t^{e+1}, \dots, t^{d-1} . As u is a prefix of U , v is a suffix of V , and $|u| = |v| = |w|$ is a proper period of s , we see that $us = sv$. Thus, we obtain a canonical homomorphism $\varphi : H' \rightarrow E(A, G)$. We have to show that φ is injective. For this it is enough to consider a Britton-reduced word in H' which begins with s or with \bar{s} . We can write this word as a sequence $s^{\varepsilon_1}y_1 \dots s^{\varepsilon_n}y_n$ with $\varepsilon_i = \pm 1$ and $y_i \in H$ for $1 \leq i \leq n$ and we may assume that $n \geq 1$.

If the word is trivial in $E(A, G)$, then it must contain a factor of the form $\bar{x}zx$ where $\deg(z) < \deg(x) = \deg(s)$, $|x|$ has leading coefficient 1, and $z = 1 \in E(A, G)$. Moreover, (by symmetry and by making x shorter if necessary) we may assume that x or \bar{x} can be depicted as $[UUU \dots](\dots WWW)$. No such factor $\bar{x}zx$ appears inside s or \bar{s} . Thus, we have $n \geq 2$ and we may assume that $\bar{x}zx$ is a factor of $s^{\varepsilon_1}y_1s^{\varepsilon_2}$. Assume that $\varepsilon_1 = \varepsilon_2$, say $\varepsilon_1 = \varepsilon_2 = 1$, then $\bar{x}zx$ appears inside

$$[UUU \dots](\dots WW \dots)(\dots VVV)y_1[UUU \dots](\dots WW \dots)(\dots VVV).$$

It is also clear that the factor z must match some factor inside the middle part $(\dots VVV)y_1[UUU \dots]$. But the word w is primitive, hence \bar{w} is no factor of ww and w is a factor of $\bar{w}\bar{w}$. Therefore this is actually impossible.

Note that the arguments remain valid even if e.g. $u = \bar{v}$ (which is the least evident case). Then $U = \bar{V}$ and infinitely many cancellations inside s^2 are possible, but nevertheless inside

$$[\bar{V}\bar{V}\bar{V}\dots)(\dots WW\dots)(\dots VVV][\bar{V}\bar{V}\bar{V}\dots)(\dots WW\dots)(\dots VVV]$$

there is no factor $\bar{x}zx$ with degree $\deg(s) = \deg(x) > \deg(z)$.

The conclusion is $\varepsilon_1 = -\varepsilon_2$ and we may assume $\varepsilon_1 = -1$. We therefore may assume that $\bar{x}zx$ is a factor inside the word $\bar{s}ys$ with $y = y_1 \in H$. Making z longer and x shorter we may assume that y is a factor of the word z , and z has the form $\bar{U}_1 y U_2$ where U_1, U_2 are prefixes of $[UUU\dots]$. Without restriction we have $U_1 = U^n$ and $|U_1| \leq |U_2|$. Since \bar{x} appears as a suffix of \bar{s} we may indeed assume that x has the form $[UUU\dots)(\dots WWW]$. The word x begins (inside the word s) with $puu\dots$, where $|p| < |u|$. More precisely, $|U_2|$ is a proper period of x , and we can write $|U_2| = \beta t^{e+1} + m|u| - |p|$ for some $\beta \in \mathbb{Z}[t]$, $m \in \mathbb{Z}$, and suffix p of u . By Lemma 7.2 $|p|$ is a proper period of x and in turn $|p|$ is a period of the word wu . Since w is primitive we conclude $p = 1$, thus $|U_2| = \beta t^{e+1} + m|u|$. In particular, U_2 ends with $(\dots uu]$ and we see that actually $U_1 = U^n$ is a suffix of U_2 . Replacing x by $U^n x$ we may assume that the factor z has the form yU' . We conclude that U' is a prefix of $[UUU\dots]$ and $U' \in H$ (because $y \in H$ and $z = 1 \in E(A, G)$).

It is now enough to show that $U' \in \langle u \rangle$. Write $|U'| \equiv \alpha \pmod{t^{e+1}}$ with $\deg(\alpha) \leq e$. Note that $|U'| = |U_2| - n|U|$ is still a proper period of x . Thus, as above we see that $\alpha = k|u|$ for some $k \in \mathbb{Z}$. This implies that U' is in the centralizer of u and U' is cyclically G -reduced. In particular, $\deg U'^m = \text{red-deg}(U'^m)$ for all $m \in \mathbb{Z}$. By hypothesis the centralizer of u is cyclic, hence for some element $r \in E(A, G)$ and some $\ell, m \in \mathbb{Z}$ we obtain $U' = r^\ell$, $u = r^m$. It follows $U'^m = u^\ell \in E(A, G)$. Hence $\deg U' \leq e = \deg(u)$, too. We conclude

$$|U'| = \alpha = k|u|.$$

As U' is a prefix of $[UUU\dots]$, we see that $U' = u^k$; and the result is shown. \square

References

- [1] R. Alperin and H. Bass. Length functions of group actions on Λ -trees. *Combinatorial group theory and topology*, 111:265–378, 1987.
- [2] H. Bass. Group actions on non-Archimedean trees. In *Arboreal group theory (Berkeley, CA, 1988)*, volume 19 of *Math. Sci. Res. Inst. Publ.*, pages 69–131. Springer, New York, 1991.

- [3] M. Bestvina and M. Feighn. Stable actions of groups on real trees. *Invent. Math.*, 121(2):287–321, 1995.
- [4] R. Book and F. Otto. *Confluent String Rewriting*. Springer-Verlag, 1993.
- [5] I. Chiswell. *Introduction to Λ -trees*. World Scientific, 2001.
- [6] I. Chiswell and T. Muller. Embedding theorems for tree-free groups. Under consideration.
- [7] V. Diekert, A. J. Duncan, and A. G. Myasnikov. Geodesic rewriting systems and pregroups. In O. Bogopolski, I. Bumagin, O. Kharlampovich, and E. Ventura, editors, *Combinatorial and Geometric Group Theory*, Trends in Mathematics, pages 55–91. Birkhäuser, 2010.
- [8] A. M. G. Baumslag and V. Remeslennikov. Residually hyperbolic groups. *Proc. Inst. Appl. Math. Russian Acad. Sci.*, 24:3–37, 1995.
- [9] D. Gaboriau, G. Levitt, and F. Paulin. Pseudogroups of isometries of \mathbb{R} and Rips’ theorem on free actions on \mathbb{R} -trees. *Israel. J. Math.*, 87:403–428, 1994.
- [10] M. Jantzen. *Confluent String Rewriting*, volume 14 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, 1988.
- [11] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. I: Irreducibility of quadratic equations and Nullstellensatz. *J. of Algebra*, 200:472–516, 1998.
- [12] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. II: Systems in triangular quasi-quadratic form and description of residually free groups. *J. of Algebra*, 200(2):517–570, 1998.
- [13] O. Kharlampovich and A. Myasnikov. Implicit function theorems over free groups. *J. of Algebra*, 290:1–203, 2005.
- [14] O. Kharlampovich and A. Myasnikov. Elementary theory of free non-abelian groups. *J. of Algebra*, 302:451–552, 2006.
- [15] O. Kharlampovich, A. Myasnikov, V. Remeslennikov, and D. Serbin. Groups with free regular length functions in \mathbb{Z}^n . To appear, arXiv:0907.2356v2.
- [16] O. Kharlampovich, A. Myasnikov, V. Remeslennikov, and D. Serbin. Subgroups of fully residually free groups: algorithmic problems. In A. G. Myasnikov and V. Shpilrain, editors, *Group theory, Statistics and Cryptography*, volume 360, pages 63–101, 2004.

- [17] R. Lyndon. Groups with parametric exponents. *Trans. Amer. Math. Soc.*, 9:518—533, 1960.
- [18] R. Lyndon and P. Schupp. *Combinatorial Group Theory*. Classics in Mathematics. Springer, 2001.
- [19] I. Lysenok. On some algorithmic problems of hyperbolic groups. *Math. USSR Izvestiya*, 35:145–163, 1990.
- [20] K. A. Mihailova. The occurrence problem for direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958. English translation in: *Math. USSR Sbornik*, 70: 241–251, 1966.
- [21] J. Morgan and P. Shalen. Valuations, trees, and degenerations of hyperbolic structures. *I. Annals of Math*, 120(3):401–476, 1984.
- [22] A. Myasnikov, V. Remeslennikov, and D. Serbin. Regular free length functions on Lyndon’s free $\mathbb{Z}[t]$ -group $F^{\mathbb{Z}[t]}$. *Contemp. Math., Amer. Math. Soc.*, 378:37–77, 2005.
- [23] A. Nikolaev. *Membership Problem in Groups Acting Freely on Non-Archimedean Trees*. Doctor of philosophy, McGill University, Montreal, Quebec, August 2010.
- [24] A. Y. Olshanskii and M. V. Sapir. Length functions on subgroups in finitely presented groups. In *Groups — Korea’98 (Pusan)*. de Gruyter, 2000.
- [25] A. Y. Olshanskii and M. V. Sapir. Length and area functions on groups and quasi-isometric Higman embeddings. *IJAC*, 11(2):137–170, 2001.
- [26] E. Rips. Subgroups of small cancellation groups. *Bull. London Math. Soc.*, 14:45–47, 1982.
- [27] N. S. Romanovskii. The occurrence problem for extensions of abelian by nilpotent groups. *Sib. Math. J.*, 21:170–174, 1980.
- [28] J.-P. Serre. *Trees*. New York, Springer, 1980.
- [29] J. Stallings. *Group theory and three-dimensional manifolds*. Yale University Press, New Haven, Conn., 1971. A James K. Whittemore Lecture in Mathematics given at Yale University, 1969, Yale Mathematical Monographs, 4.

Volker Diekert, Universität Stuttgart, Universitätsstr. 38, 70569 Stuttgart, Germany
 Alexei Myasnikov, Stevens Institute of Technology, Hoboken, NJ 07030, USA

Group extensions over infinite words*

Volker Diekert

Alexei Myasnikov

February 8, 2011

Abstract

We construct an extension $E(A, G)$ of a given group G by infinite non-Archimedean words over a discretely ordered abelian group like \mathbb{Z}^n . This yields an effective and uniform method to study various groups that "behave like G ". We show that the Word Problem for finitely generated subgroups in the extension is decidable if and only if the Cyclic Membership Problem in G is decidable. The present paper embeds the partial monoid of infinite words as defined by Myasnikov, Remeslennikov, and Serbin in [22] into $E(A, G)$. Moreover, we define the extension group $E(A, G)$ for arbitrary groups G and not only for free groups as done in previous work. We show some structural results about the group (existence and type of torsion elements, generation by elements of order 2) and we show that some interesting HNN extensions of G embed naturally in the larger group $E(A, G)$.

1 Introduction

In this paper we construct an extension of a given group G by infinite non-Archimedean words. The construction is effective and gives a new uniform method to study various groups that "behave like G ": limits of G in the Gromov-Hausdorff topology, fully residually G groups, groups obtained from G by free constructions, etc. Infinite non-Archimedean words appeared first in [22] in connection with group actions on trees. The fundamentals for group actions on simplicial trees (now known as Bass-Serre theory) were laid down by Serre in his seminal book [28].

*Part of the work has been started in 2007 when the authors were at the CRM (Centro Recherche Matemàtica, Barcelona). It was finished when the first author stayed at Stevens Institute of Technology in September 2010. The support of both institutions is greatly acknowledged

General Λ -trees for ordered abelian groups Λ were introduced by Morgan and Shalen in [21] and their theory was further developed by Alperin and Bass in [1]. The Archimedean case concerns with group actions on \mathbb{R} -trees.

A complete description of finitely generated groups acting freely on \mathbb{R} -trees was obtained in a series of papers [3, 9]. It is known now as Rips' Theorem, see [5] for a detailed discussion.

For non-Archimedean actions much less is known. Much of the recent progress is due to Chiswell and Müller [6], Kharlampovich, Myasnikov, Remeslennikov, and Serbin [16, 15, 22] and the recent thesis of Nikolaev [23]. In these papers groups acting on freely on \mathbb{Z}^n -trees are represented as words where the length takes values in the ring of integer polynomials $\mathbb{Z}[t]$. More precisely, in [22] the authors represent elements of Lyndon's free $\mathbb{Z}[t]$ -group $F^{\mathbb{Z}[t]}$ (the free group with basis Σ and exponentiation in $\mathbb{Z}[t]$) by infinite words, which are defined as mappings $w : [1, \alpha] \rightarrow \Sigma^{\pm 1}$ over closed intervals $[1, \alpha] = \{\beta \in \mathbb{Z}[t] \mid 1 \leq \beta \leq \alpha\}$. Here, the ring $\mathbb{Z}[t]$ is viewed as an ordered abelian group in the standard way: $0 < \alpha$ if the leading coefficient of the polynomial α is positive. This yields a regular free Lyndon length function with values in $\mathbb{Z}[t]$.

The importance of Lyndon's group $F^{\mathbb{Z}[t]}$ became also prominent due to its relation to algebraic geometry over groups and the solution of the Tarski Problems [11, 12, 13, 14]. It was known by [8] and the results above that finitely generated fully residually free groups are embeddable into $F^{\mathbb{Z}[t]}$. The converse (every finitely generated subgroup of $F^{\mathbb{Z}[t]}$ is fully residually free) was shown in the original paper by Lyndon [17]. It follows that every finitely generated fully residually free group has a free length function with values in a free abelian group of finite rank with the lexicographic order. It turned out that the representation of group elements as infinite words over $\mathbb{Z}[t]$ is quite intuitive and it enables a *combinatorics on words* similar to finite words. This technique leads to the solution of various algorithmic problems for $F^{\mathbb{Z}[t]}$ using the standard Nielsen cancellation argument for the length function.

This concept is the starting point for our paper: We use finite words over $\Sigma^{\pm 1}$ to represent elements of G . Then, exactly as in the earlier papers mentioned above, an infinite word is a mapping $w : [1, \alpha] \rightarrow \Sigma^{\pm 1}$ over a closed interval $[1, \alpha] = \{\beta \in \mathbb{Z}[t] \mid 1 \leq \beta \leq \alpha\}$. The monoid of infinite words is endowed with a natural involution. We can read $w : [1, \alpha] \rightarrow \Sigma^{\pm 1}$ from right-to-left and simultaneously we inverse each letter. This defines \bar{w} . Clearly, $\bar{\bar{w}} = w$ and $\overline{uv} = \bar{v}\bar{u}$. The naive idea is to use now $w\bar{w} = 1$ as defining relations in order to obtain a group. This idea falls short drastically, because the group collapses. The image of the $F(\Sigma)$ in this group is $\mathbb{Z}/2\mathbb{Z}$ (for $\Sigma \neq \emptyset$). Therefore the set of infinite words was viewed as a partial monoid, only. It was shown that $F^{\mathbb{Z}[t]}$ embeds into this partial monoid, but the proof is complicated and demands technical tools.

The first major deviation in our approach (from what has been done so far) is

that we still work with equations $w\bar{w} = 1$, but we restrict them to freely reduced words w . Just as in the finite case: A word w is called freely reduced, if no factor aa^{-1} (where a is a letter) appears. This means, there is no $1 < \beta < \alpha$ such that $w(\beta) = w(\beta + 1)^{-1}$. The submonoid generated by freely reduced words (inside the monoid of all infinite words) modulo defining equations $w\bar{w} = 1$ defines a group (which is trivial) where $F(\Sigma)$ embeds (which is non-trivial). Actually, $F^{\mathbb{Z}[t]}$ embeds. It turns out that many freely reduced words satisfy $\bar{w} = w$. Thus, the involution has fixed points, and many elements have 2-torsion in our group. Actually, in natural situations the group is generated by these elements of order 2.

Our focus is more ambitious and goes beyond extending free groups $F(\Sigma)$. We begin with an arbitrary group G generated by Σ . This gives rise to the notion of a G -reduced word. An $\mathbb{Z}[t]$ -word is G -reduced, if no finite factor $w[\beta, \beta + m]$ with $m \in \mathbb{N}$ represents the unit element 1 in G . We let $R^*(A, G)$ denote the submonoid generated by G -reduced words (inside the monoid of all infinite words) where $A = \mathbb{Z}[t]$. Clearly, we may assume that $R^*(A, G)$ contains all finite words (because we may assume that all letters are G -reduced). Then we factor out defining equations for G (which are words in $\Sigma^{\pm 1}$) and defining equations $u\bar{u} = 1$ with $u \in R^*(A, G)$. In this way we obtain a group denoted here by $E(A, G)$.

The first main result of the paper states that G embeds into $E(A, G)$, see Corollary 5.5. The result is obtained by the proof that some (non-terminating) rewriting system is strongly confluent, thus confluent. This is technically involved and covers all of Section 5.

The second main result concerns the question when the Word Problem is decidable in all finitely generated subgroups of $E(A, G)$. An obvious precondition is that the base group G itself must share this property. However, this is not enough and makes the situation somehow non-trivial. We show in Corollary 8.5 that the Word Problem is decidable in all finitely generated subgroups of $E(A, G)$ if and only if the Cyclic Membership Problem " $u \in \langle v \rangle$?" is decidable for all $v \in G$. There are known examples where G has a soluble Word Problem, but Cyclic Membership Problem is not decidable for some specific v , see [24, 25]. On the other hand, the Cyclic Membership Problem is uniformly decidable in many natural classes (which encompasses classes of groups with decidable Membership Problem w.r.t. subgroups) like hyperbolic groups, one-relator groups or effective HNN-extensions, see Remark 8.8.

In the final section we show that the partial monoid $\text{CDR}(A, \Sigma)$ of infinite words with a cyclically reduced decompositions (c.f. [22]) embeds in our group $E(A, G)$, and we show that some interesting HNN extensions can be embedded into $E(A, G)$ as well which are not realizable inside the partial monoid $\text{CDR}(A, \Sigma)$, Proposition 9.4. In order to achieve this result we show that every cyclically G -reduced word in $E(A, G)$ sits inside a free abelian subgroup of infinite rank, Proposition 9.3.

The proof techniques in this paper are of combinatorial flavor and rely on the theory of rewriting systems. No particular knowledge on non-Archimedean words or groups acting on \mathbb{Z}^n -trees is required.

2 Preliminaries on rewriting techniques

Rewriting techniques are a convenient tool to prove that certain constructions have the expected properties. Typically we extend a given group by new generators and defining equations and we want that the original group embeds in the resulting quotient structure. For example, HNN extensions and amalgamated products or Stallings's embedding (see [29]) of a pregroup in its universal group can be viewed from this viewpoint, [7]. Here we use them in the very same spirit. First, we recall the basic concepts.

A *rewriting relation* over a set X is binary a relation $\Longrightarrow \subseteq X \times X$. By $\xRightarrow{+}$ ($\xRightarrow{*}$ resp.) we mean the transitive (reflexive and transitive resp.) closure of \Longrightarrow . By $\xLeftrightarrow{*}$ ($\xLeftrightarrow{*}$ resp.) we mean the symmetric (symmetric, reflexive, and transitive resp.) closure of \Longrightarrow . We also write $y \xLeftarrow{*} x$ whenever $x \xRightarrow{*} y$, and we write $x \xRightarrow{\leq k} y$ whenever we can reach y in at most k steps from x .

Definition 2.1. *The relation $\Longrightarrow \subseteq X \times X$ is called:*

- i.) *strongly confluent, if $y \xLeftarrow{*} x \xRightarrow{*} z$ implies $y \xRightarrow{\leq 1} w \xLeftrightarrow{\leq 1} z$ for some w ,*
- ii.) *confluent, if $y \xLeftarrow{*} x \xRightarrow{*} z$ implies $y \xRightarrow{*} w \xLeftarrow{*} z$ for some w ,*
- iii.) *Church-Rosser, if $y \xLeftrightarrow{*} z$ implies $y \xRightarrow{*} w \xLeftarrow{*} z$ for some w ,*
- iv.) *locally confluent, if $y \xLeftarrow{*} x \xRightarrow{*} z$ implies $y \xRightarrow{*} w \xLeftarrow{*} z$ for some w ,*
- v.) *terminating, if every infinite chain*

$$x_0 \xRightarrow{*} x_1 \xRightarrow{*} \cdots x_{i-1} \xRightarrow{*} x_i \xRightarrow{*} \cdots$$

becomes stationary,

- vi.) *convergent (or complete), if it is locally confluent and terminating.*

The following facts are well-known, proofs are easy and can be found in any text book on rewriting systems, see e.g. [4, 10].

Proposition 2.2. *The following assertions hold:*

1. *Strong confluence implies confluence.*
2. *Confluence is equivalent with Church-Rosser.*
3. *Confluence implies local confluence, but the converse is false, in general.*
4. *Convergence (i.e., local confluence and termination together) implies confluence.*

Often one is interested in the case, only where X is a free group or a free monoid and the rewriting relation is specified by directing defining equations. Here we are more general in the following sense. Let M be any monoid. A *rewriting system* over M is a relation $S \subseteq M \times M$. Elements $(\ell, r) \in S$ are also called *rules*. The system S defines the rewriting relation $\xRightarrow[S]{*} \subseteq M \times M$ by

$$x \xRightarrow[S]{*} y, \text{ if } x = p\ell q, y = prq \text{ for some rule } (\ell, r) \in S.$$

The relation $\xRightarrow[S]{*} \subseteq M \times M$ is a congruence, hence the congruence classes form a monoid which is denoted by $M / \{\ell = r \mid (\ell, r) \in S\}$. Frequently we simply write M/S for this quotient monoid. Notice, that if M is a free monoid with basis X then M/S is the monoid given by the presentation $\langle X \mid \ell = r, \text{ where } (\ell, r) \in S \rangle$.

We say that S is strongly confluent or confluent etc, if in fact $\xRightarrow[S]{*}$ has the corresponding property. Instead of $(\ell, r) \in S$ we also write $\ell \rightarrow_S r \in S$ and $\ell \leftarrow_S r \in S$ in order to indicate that both $(\ell, r) \in S$ and $(r, \ell) \in S$. By $\text{IRR}(S)$ we mean the set of *irreducible normal forms*. This is the subset of M where no rule of S can be applied, i.e.,

$$\text{IRR}(S) = M \setminus \bigcup_{(\ell, r) \in S} M\ell M.$$

If S is terminating, then we have $1 \in \text{IRR}(S)$, and if S is convergent, then the canonical homomorphism $M \rightarrow M/S$ induces a bijection between $\text{IRR}(S)$ and the quotient monoid M/S .

If a quotient monoid is given by a finite convergent string rewriting system $S \subseteq \Gamma^* \times \Gamma^*$, then the monoid has a decidable Word Problem, which yields a major interest in these systems.

Example 2.3. *Let Σ be a set and Σ^{-1} be disjoint copy. Then the set of rules $\{aa^{-1} \rightarrow 1, a^{-1}a \rightarrow 1 \mid a \in \Sigma\}$ defines a strongly confluent and terminating system over $(\Sigma \cup \Sigma^{-1})^*$ which defines the free group $F(\Sigma)$ with basis Σ .*

In this paper however, we will deal mainly with non-terminating systems which are moreover in many cases infinite. So convergence plays a minor role here. There is another class of string rewriting systems which for finite systems leads to a polynomial space (and hence exponential time in the worst case) decision algorithm for the Word Problem.

Definition 2.4. A string rewriting system $S \subseteq \Gamma^* \times \Gamma^*$ is called pre-perfect, if the following three conditions hold:

1. The system S is confluent.
2. If we have $\ell \rightarrow r \in S$, then we have $|\ell| \geq |r|$ where $|x|$ denotes the length of a word x .
3. If we have $\ell \rightarrow r \in S$ with $|\ell| = |r|$, then we have $r \rightarrow \ell \in S$, too.

Clearly, a convergent length-reducing system is pre-perfect, and if a confluent system satisfies $|\ell| \geq |r|$ for all $\ell \rightarrow r \in S$, then we can add symmetric rules in order to make it pre-perfect.

3 Non-Archimedean words

We consider group extensions over infinite words of a specific type. These words are also called *non-Archimedean words*, because they are defined over non-archimedean ordered abelian groups.

3.1 Discretely ordered abelian groups

A *ordered abelian group* is an abelian group A together with a linear order \leq such that $x \leq y$ if and only if $x + z \leq y + z$ for all $x, y, z \in A$. It is *discretely ordered*, if in addition there is least positive element 1_A . Here, as usual, an element x is *positive*, if $0 < x$. An ordered abelian group is *Archimedean*, if for all $0 \leq a \leq b$ there is some $n \in \mathbb{N}$ such that $b < na$, otherwise it is *non-Archimedean*.

If B is any ordered abelian group, then $A = \mathbb{Z} \times B$ is discretely ordered with $1_A = (1, 0)$ and the lexicographical ordering:

$$(a, b) \leq (c, d) \text{ if } b < d \text{ or } b = d \text{ and } a \leq c.$$

The group is non-Archimedean unless B is trivial since $(n, 0) < (0, x)$ for all $n \in \mathbb{N}$ and positive $x \in B$.

In particular, $\mathbb{Z} \times \mathbb{Z}$ is a non-Archimedean discretely ordered abelian group. It serves as our main example. Iterating the process all finitely generated free

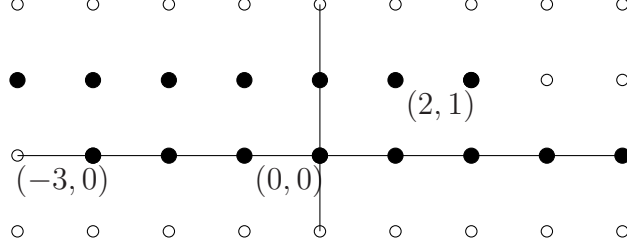


Figure 1: A closed interval of length $(6, 1)$ in $\mathbb{Z} \times \mathbb{Z}$

abelian \mathbb{Z}^k are viewed as being discretely ordered; and by a transfinite iteration we can consider arbitrary direct sums of \mathbb{Z} . This is where we limit ourselves. In this paper we consider discretely ordered abelian groups only, which can be written as

$$A = \oplus_{i \in \Omega} \langle t_i \rangle, \quad (1)$$

where Ω is a set of ordinals, and $\langle t_i \rangle$ denotes the infinite cyclic group \mathbb{Z} generated by the element t_i . Elements of A are finite sums $\alpha = \sum_i n_i t_i$ with $n_i \in \mathbb{Z}$. Since the sum is finite, either $\alpha = 0$ or there is a greatest ordinal $i \in \Omega$ (denoted by $\deg(\alpha)$) with $n_i \neq 0$. By convention, $\deg(0) = -\infty$. We call $\deg(\alpha)$ the *degree* or *height* of α . An element $\alpha = \sum_i n_i t_i \in A$ is called *positive*, if $n_d > 0$ for $d = \deg(\alpha)$. We let $\alpha \leq \beta$, if $\alpha = \beta$ or $\beta - \alpha$ is positive. Moreover, for $\alpha, \beta \in A$ we define the *closed interval* $[\alpha, \beta] = \{\gamma \in A \mid \alpha \leq \gamma \leq \beta\}$. Its *length* is defined to be $\beta - \alpha + 1$.

For $\mathbb{Z} \times \mathbb{Z}$ the interval $[(-3, 0), (2, 1)]$ is depicted as in Fig. 1. Its length is $(6, 1)$.

Sometimes we simply illustrate intervals of length $(m, 1)$ as \dots and intervals of length $(m, 2)$ as $\dots(\dots)$. This will become clearer later.

3.2 Non-Archimedean words over a group G

An *involution* of a set M is a mapping $M \rightarrow M, x \mapsto \bar{x}$ with $\bar{\bar{x}} = x$ for all $x \in M$. A *monoid with involution* is a monoid M with an involution $x \mapsto \bar{x}$ such that $\overline{xy} = \bar{y}\bar{x}$ for all $x, y \in M$ and, as a consequence, $\bar{1} = 1$. Every group is a monoid with involution $x \mapsto x^{-1}$. Obviously, if M is a monoid with involution $x \mapsto \bar{x}$ then the quotient $M / \{x\bar{x} = 1 \mid x \in M\}$ is a group. Furthermore, if G is a group and M is a monoid with involution then every monoid homomorphism respecting involutions $\varphi : M \rightarrow G$ factors through this canonical quotient. Let

$a \mapsto \bar{a}$ denote a bijection between sets Σ and $\bar{\Sigma}$, hence $\bar{\Sigma} = \{\bar{a} \mid a \in \Sigma\}$. The map $a \mapsto \bar{a}, \bar{a} \mapsto a$ is an involution on $\Sigma \cup \bar{\Sigma}$ with $\bar{\bar{a}} = a$. It extends to an involution $x \mapsto \bar{x}$ on the free monoid $(\Sigma \cup \bar{\Sigma})^*$ with basis $\Sigma \cup \bar{\Sigma}$ by $\overline{a_1 \cdots a_n} = \bar{a}_n \cdots \bar{a}_1$. In case that $\Sigma \cap \bar{\Sigma} = \emptyset$ the resulting structure $((\Sigma \cup \bar{\Sigma})^*, \cdot, 1, \bar{\cdot})$ is the *free monoid with involution* with basis Σ .

Throughout G denotes a group with a generating set Σ . We always assume that $a \neq 1$ for all $a \in \Sigma$. We let $\Gamma = \Sigma \cup \bar{\Sigma}$, where $\bar{\Sigma} = \Sigma^{-1} \subseteq G$ and $\bar{a} = a^{-1}$ for $a \in \Gamma$. The inclusion $\Gamma \subseteq G$ induces the canonical homomorphism (presentation) onto the group G :

$$\pi : \Gamma^* \rightarrow G.$$

Clearly, for every word $w \in \Gamma^*$ we have $\pi(\bar{w}) = \pi(w)^{-1}$. Note that there are fixed points for the involution on Γ in case Σ contains an element of order 2.

Let $A = \oplus_{i \in \Omega} \langle t_i \rangle$ be a discretely ordered abelian group as above. A *partial A-map* is a map $p : D \rightarrow \Gamma$ with $D \subseteq A$. Two partial maps $p : D \rightarrow \Gamma$ and $p' : D' \rightarrow \Gamma$ are termed equivalent if p' is an α -shift of p for some $\alpha \in A$, i.e., $D' = \{\alpha + \beta \mid \beta \in D\}$ and $p'(\alpha + \beta) = p(\beta)$ for all $\beta \in D$. This an equivalence relation on partial A -maps, and an equivalence class of partial A -maps is called a *partial A-word*. If $D = [\alpha, \beta] = \{\gamma \in A \mid \alpha \leq \gamma \leq \beta\}$ then the equivalence class of $p : [\alpha, \beta] \rightarrow \Gamma$ is called a *closed A-word*. By abuse of language a closed (resp. partial) A -word is sometimes simply called a *word* (resp. *partial word*).

A word $p : [\alpha, \beta] \rightarrow \Gamma$ is *finite* if the set $[\alpha, \beta]$ is finite, otherwise it is *infinite*. Usually, we identify finite words with the corresponding elements in Γ^* .

If $p : [\alpha, \beta] \rightarrow \Gamma$ and $q : [\gamma, \delta] \rightarrow \Gamma$ are closed A -words, then we define their concatenation as follows. We may assume that $\gamma = \beta + 1$ and we let:

$$\begin{aligned} p \cdot q : [\alpha, \delta] &\rightarrow \Gamma \\ x &\mapsto p(x) && \text{if } x \leq \beta \\ x &\mapsto q(x) && \text{otherwise.} \end{aligned}$$

It is clear that this operation is associative. Hence, the set of closed A -words forms a monoid, which we denote by $W(A, \Gamma)$. The neutral element, denoted by 1, is the totally undefined mapping. The standard representation of an A -word p is a mapping $p : [1, \alpha] \rightarrow \Gamma$, where $0 \leq \alpha$. In this case α is called the *length* of p ; sometimes we also write $|p| = \alpha$. The *height* or *degree* of p is the degree of α ; we also write $\deg(p) = \deg(\alpha)$. For a partial word $p : D \rightarrow \Gamma$ and $[\alpha, \beta] \subseteq D$ we denote by $p[\alpha, \beta]$ the restriction of p to the interval $[\alpha, \beta]$. Hence $p[\alpha, \beta]$ is a closed word. Sometimes we write $p[\alpha]$ instead of $p[\alpha, \alpha]$. Thus, $p[\alpha] = p(\alpha)$.

The monoid $W(A, \Gamma)$ is a monoid with involution $p \mapsto \bar{p}$ where for $p : [1, \alpha] \rightarrow \Gamma$ we define $\bar{p} \in W(A, \Gamma)$ by $\bar{p} : [-\alpha, -1] \rightarrow \Gamma, -\beta \mapsto p(\beta)$.

Recall that $A = \oplus_{i \in \Omega} \langle t_i \rangle$. We may assume that 0 is the least ordinal in Ω , in which case \mathbb{Z} can be viewed as a subgroup of A via the embedding $n \mapsto nt_0$. Thus $1 \in \mathbb{N}$ is also the smallest positive element in A . If, for example, $A = \mathbb{Z} \times \mathbb{Z}$, then we have identified $1 \in \mathbb{N}$ with the pair $(1, 0)$.

If $x \in W(A, \Gamma)$ and $x = pfq$ for some $p, q \in W(A, \Gamma)$ then p is called a *prefix*, q is called a *suffix*, and f is called a *factor* of x . If $1 \neq f \neq x$ then f is called a *proper factor*. As usual, a factor is finite, if $|f| \in \mathbb{N}$. Thus, a finite factor can be written as $x[\alpha, \beta]$ where $\beta = \alpha + n$, $n \in \mathbb{N}$.

A closed word $x : [1, \alpha] \rightarrow \Gamma$ is called *freely reduced* if $x(\beta) \neq \overline{x(\beta + 1)}$ for all $1 \leq \beta < \alpha$. It is called *cyclically reduced* if x^2 is freely reduced.

As a matter of fact we need a stronger conditions. The word x is called *G-reduced*, if no finite factor $x[\alpha, \alpha + n]$ with $n \in \mathbb{N}$, $n \geq 1$, becomes the identity 1 in the group G . Note that all *G-reduced* words are freely reduced by definition. We say x is *cyclically G-reduced*, if every finite power x^k with $k \in \mathbb{N}$ is *G-reduced*. Over a free group G with basis Σ a word is freely reduced if and only if it is *G-reduced*, and it is cyclically *G-reduced* if and only if it is cyclically reduced.

In Fig. 2 we see a closed word which is not freely reduced. Fig. 3 defines a word w with a sloppy notation $[aaa \cdots)(\cdots abab \cdots)(\cdots bbb]$. Fig. 4 shows that for the same word w we have $aw \neq wb$ (because $aw[(0, 1)] = a$ and $wb[(0, 1)] = b$), but we have $aaw = wbb$ in the monoid $W(A, \Gamma)$, see Fig. 5. Recall, that two elements x, y in a monoid M are called *conjugated*, if $xw = wy$ for some $w \in M$. Fig. 6 shows that all finite words $x, y \in \Gamma^*$ are conjugated in $W(A, \Gamma)$ provided they have the same length $|x| = |y|$ and A is non-Archimedean. Indeed $t = [uuu \cdots)(\cdots vvv]$ does the job $ut = tv$. Clearly, $ut = tv$ implies $|x| = |y|$. In particular, this shows that the monoid $W(A, \Gamma)$ is not free. Indeed, if x and y are conjugated elements in a free monoid, say $xw = wy$, then $x = rs$, $y = sr$, and $w = (rs)^m r$ for some $r, s \in \Gamma^*$ and $m \in \mathbb{N}$, which is not the case for the example above.

If G is an infinite group, then there are *G-reduced* A -words of arbitrary length.

Lemma 3.1. *Let G be an infinite group and $\alpha \in A$. Then there exists a *G-reduced* A -word $x : [1, \alpha] \rightarrow \Gamma$ of length α .*

Proof. First, let us assume that Γ is finite. We may assume that letters of Γ are *G-reduced*. There are infinitely many finite *G-reduced* words in Γ^* , simply because each group element can be represented this way. They form a tree in the following way. The root is the empty word 1. A letter has 1 as its parent node. A finite *G-reduced* word of the form $w = avb$ with $a, b \in \Gamma$ has v as its parent node. Since Γ is finite the degree of each node is finite. Hence König's Lemma tells us that there must be an infinite path. Following this path from the root yields a partial word $p : \mathbb{Z} \rightarrow \Gamma$ in an obvious way: If v denotes the *G-reduced* word $v : [m, n] \rightarrow \Gamma$, then $w = avb$ denotes the *G-reduced* word $w : [m - 1, n + 1] \rightarrow \Gamma$



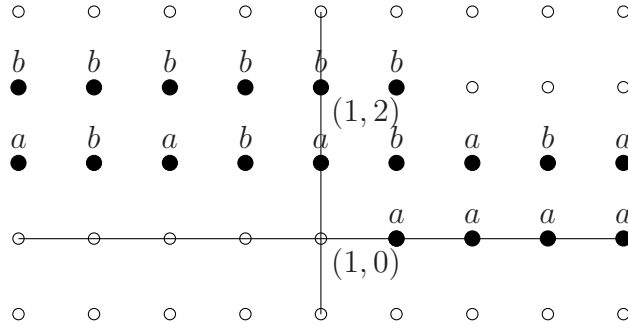


Figure 4: $aw = a[aaa \dots](\dots abab \dots)(\dots bbb)$ and $aw \neq wb$.

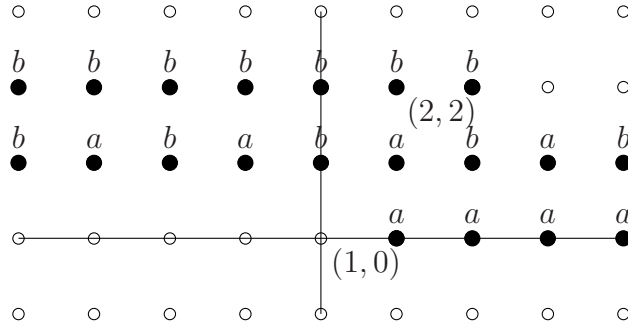


Figure 5: $aa[aaa \dots](\dots abab \dots)(\dots bbb)bb = [aaa \dots](\dots abab \dots)(\dots bbb)bb$

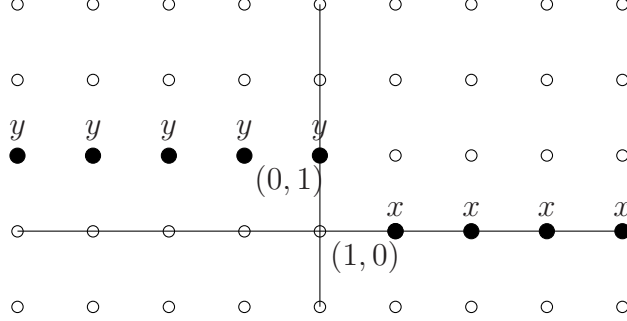


Figure 6: An infinite word $t = [xxx \cdots](\cdots yyy]$ where $xt = ty$.

with $w[m-1] = a$, $w[m, n] = v$, and $w[n+1] = b$. This mapping $p : \mathbb{Z} \rightarrow \Gamma$ can be extended to a mapping $q : A \rightarrow \Gamma$ by $q(\sum_i n_i t_i) = p(n_0)$. This means we project $\alpha \in A$ to the first component and then we use p . For every $\alpha \in A$ the partial word $q[1, \alpha] \rightarrow \Gamma$ is G -reduced.

If G is finitely generated but Γ is infinite then one can repeat the argument above for some large enough finite subset of Γ (that generates G). It remains to consider the case that G is not finitely generated. Assume a G -reduced word $v : [m, n] \rightarrow \Gamma$ has been constructed. Then we choose $a \in \Gamma$ such that a is not in subgroup generated by the elements $v[i]$ for $m \leq i \leq n$. Clearly, $av : [m-1, n] \rightarrow \Gamma$ is G -reduced. Next choose $b \in \Gamma$ such that b is not in subgroup generated by the elements $av[i]$ for $m-1 \leq i \leq n$. Now, $avb : [m-1, n+1] \rightarrow \Gamma$ is G -reduced. We obtain a G -reduced word $p : \mathbb{Z} \rightarrow \Gamma$ and we argue as above. \square

By $R(A, G)$ we denote the set of all G -reduced words in $W(A, \Gamma)$, and by $R^*(A, G)$ we mean the submonoid of $W(A, \Gamma)$ which is generated by $R(A, G)$.

Remark 3.2. *In the notation above:*

- If the group G is finite, then $R(A, G)$ cannot contain any infinite word, and in this case $R^*(A, G) = \Gamma^*$.
- If $A = \mathbb{Z}$ then $W(\mathbb{Z}, \Gamma) = \Gamma^*$.

These situations are without any interest in our context, so we assume in the sequel that G is infinite and that A has rank at least 2 (i.e., it is non-Archimedean).

Observe, that the length function $W(A, \Gamma) \rightarrow A, p \mapsto |p|$ induces a canonical homomorphism onto $\oplus_{i \in \Omega} \mathbb{Z}/2\mathbb{Z}$ which therefore factors through the greatest

quotient group of $W(A, \Gamma)$. This group collapses Σ into a group of order 2, and therefore the greatest quotient group of $W(A, \Gamma)$ is of no particular interest here. More precisely, we have the following fact.

Proposition 3.3. *Let $\Sigma \neq \emptyset$ and*

$$\psi : F(\Sigma) \rightarrow W(A, \Gamma) / \{u\bar{u} = 1 \mid u \in W(A, \Gamma)\}$$

be the canonical homomorphism induced by $\Sigma \subseteq W(A, \Gamma)$, and let A have rank at least 2. Then the image of $F(\Sigma)$ under ψ is the group $\mathbb{Z}/2\mathbb{Z}$.

Proof. The image of $F(\Sigma)$ is not trivial, because it is non-trivial in the group $\oplus_{i \in \Omega} \mathbb{Z}/2\mathbb{Z}$. It is therefore enough to show that $\psi(ab) = 1$ for all $a, b \in \Gamma$. Consider the following closed word u of length $(0, 1)$:

$$u = [ababab \cdots](\cdots a\bar{a}a\bar{a}a\bar{a})$$

In $W(A, \Gamma)$ we have $abu = ua\bar{a}$. Now, $\psi(a\bar{a}) = 1$ implies $\psi(ab) = 1$. \square

Continuing with $F(\Sigma)$, consider the following word w of length $(0, 2)$, which is product of two freely reduced words where $a, b \in \Gamma$ with $a \neq \bar{b}$:

$$w = [aaa \cdots](\cdots aaa) \cdot [\bar{a}\bar{a}\bar{a} \cdots](\cdots bbb)$$

It is natural to allow (and we will do) the cancellation of factors $a\bar{a}$ inside w . The shape of the word remains the same, but the length is decreasing to any value $(-2n, 2)$ with $n \in \mathbb{N}$. If next we wish to embed $F(\Sigma)$ into any quotient structure of $W(A, \Gamma)$, then we cannot cancel however the whole middle part $(\cdots aaa) \cdot [\bar{a}\bar{a}\bar{a} \cdots]$, i.e., w cannot become equal to $v = [aaa \cdots](\cdots bbb)$ in this quotient. Indeed, assume by contradiction $w = v$, then:

$$\begin{aligned} aav = avb &= a[aaa \cdots](\cdots bbb)b \\ &= awb \\ &= [aaa \cdots](\cdots aaa) \cdot a\bar{a} \cdot [\bar{a}\bar{a}\bar{a} \cdots](\cdots bbb) \\ &= w = v. \end{aligned}$$

This implies $a^2 = 1$, a contradiction.

4 The group $E(A, G)$

Proposition 3.3 shows that, in general, the free group $F(\Sigma)$ does not naturally embed into the greatest quotient group of $W(A, \Gamma)$. Nevertheless, in this section we modify the construction to be able to represent a group G by infinite words

from $W(A, \Gamma)$. As above, we let G be a group generated by Σ and $\pi : \Gamma^* \rightarrow G$ be the induced presentation with $\Gamma = \Sigma \cup \Sigma^{-1}$. Recall that $R(A, G)$ denotes the set of closed G -reduced words, i.e.:

$$R(A, G) = \{u \in W(A, \Gamma) \mid u \text{ is } G\text{-reduced}\}.$$

Let $\mathcal{M}(A, G)$ be the following quotient monoid of $W(A, \Gamma)$:

$$\mathcal{M}(A, G) = W(A, \Gamma) / \{u\ell\bar{r}\bar{u} = 1 \mid u \in R(A, G), \ell, r \in \Gamma^*, \pi(\ell) = \pi(r)\}.$$

Definition 4.1. We define $E(A, G)$ as the image of $R^*(A, G)$ in $\mathcal{M}(A, G)$ under the canonical epimorphism $W(A, \Gamma) \rightarrow \mathcal{M}(A, G)$.

In the following proposition we collect some simple results on $E(A, G)$.

Proposition 4.2. Let G be a group generated by a set Σ and $A = \bigoplus_{i \in \Omega} \langle t_i \rangle$ as above. Then:

- 1) $E(A, G)$ is a group (a subgroup of $\mathcal{M}(A, G)$);
- 2) every submonoid of $\mathcal{M}(A, G)$ which is a group sits inside the group $E(A, G)$, so $E(A, G)$ is the group of units in $\mathcal{M}(A, G)$;
- 3) the inclusion $\Gamma \subseteq G$ induces a homomorphism $\pi^A : G \rightarrow E(A, G)$.

Proof. To see 1) observe that every element in $u \in R(A, G)$ has \bar{u} as an inverse in $E(A, G)$, so $E(A, G)$ is a group.

Notice that only the trivial word is invertible in $W(A, \Gamma)$ since concatenation does not decrease the length. Hence every equality $w\bar{w} = 1$ for a non-trivial w in $W(A, \Gamma)$ comes from the defining relations in $\mathcal{M}(A, G)$. Observe, that the defining relations are applicable only to words from $R^*(A, G)$, the set $R^*(A, G)$ is closed under such transformations. This shows that $E(A, G)$ is the group of units in $\mathcal{M}(A, G)$, as claimed in 2).

3) is obvious since $G = \Gamma^* / \{\ell\bar{r} = 1 \mid \pi(\ell) = \pi(r)\}$ and $1 \in R(A, G)$. \square

Several important remarks are due here.

- It is far from obvious that the homomorphism $\pi^A : G \rightarrow E(A, G)$ is injective. However, this is true and we prove it later in Corollary 5.5.
- It is not claimed that the definition of $\mathcal{M}(A, G)$ (or $E(A, G)$) is independent of the choice of Γ and π , but our main results hold through for any such Γ and π thus justifying the (sloppy) notations $\mathcal{M}(A, G)$ and $E(A, G)$.

- If $G = F(\Sigma)$ is the free group with basis Σ , then the definition of $\mathcal{M}(A, G)$ can be rephrased by saying that it is the quotient monoid of $W(A, \Gamma)$ with defining equations $u\bar{u} = 1$ for all freely reduced closed words u .
- It is not true in general that $E(A, G)$ can be defined as the quotient group

$$E(A, F(\Sigma)) / \{ \ell = r \mid \ell, r \in \Gamma^*, \pi(\ell) = \pi(r) \}.$$

Indeed, let r be a cyclically reduced word of length m such that $r = 1$ in G . In $E(A, F(\Sigma))$ for every $a \in \Gamma$ the words a^m and r are conjugated since

$$a^m [a^m a^m a^m \dots] (\dots rrr) = [a^m a^m a^m \dots] (\dots rrr) r.$$

Therefore, $a^m = 1$ in $E(A, F(\Sigma)) / \{ \ell = r \mid \ell, r \in \Gamma^*, \pi(\ell) = \pi(r) \}$, which may not be the case in G (which is a subgroup of $E(A, G)$).

Nevertheless, $E(A, F(\Sigma))$ satisfies some universal property.

Proposition 4.3. *Every group G generated by Σ is isomorphic to the canonical quotient of the subgroup in $E(A, F(\Sigma))$ generated by $R(A, G)$.*

Proof. The statement is obvious. □

5 Confluent rewriting systems over non-Archimedean words

Our goal here is to construct a confluent rewriting system S over the monoid $W(A, \Gamma)$ such that

$$\mathcal{M}(A, G) = W(A, \Gamma) / S$$

and S has the following form:

$$S = S_0 \cup \{ u\bar{u} \rightarrow 1 \mid u \in R(A, G) \text{ and } u \text{ is infinite} \}, \quad (2)$$

where $S_0 \subseteq \Gamma^* \times \Gamma^*$ is a rewriting system for G satisfying the following conditions:

1. $\Gamma^* / S_0 = G$
2. For all $a \in \Gamma$ we have $(a\bar{a}, 1) \in S_0$.
3. If $(\ell, r) \in S_0$, then $(\bar{\ell}, \bar{r}) \in S_0$.
4. $1 \in \Gamma^*$ is S_0 -irreducible.

5. S_0 is confluent.

In general, S_0 is neither finite nor terminating, but these conditions are not crucial for the moment, so we do not care.

Lemma 5.1. *For any group G generated by Σ there is a rewriting system $S_0 \subseteq \Gamma^* \times \Gamma^*$ satisfying the conditions 1-5 above. Moreover, if G is finitely presented, then one can choose S_0 to be finite.*

Proof. Let $G = \Gamma^*/R$ for some set of defining relation R . In general, let S_0 be the set of all rules $u \rightarrow v$, where u is non-empty and $u \neq v$ as words, but $u = v$ in G . Notice that there are no rules $1 \rightarrow r$ in S_0 , so $1 \in \text{IRR}(S_0)$. However, for every $r \in R \cup \overline{R}$ and every letter $a \in \Sigma$ the relations $a \rightarrow ra$ and $a \rightarrow ar$ are in S_0 , so one can insert any relation r in a word, thus simulating the rule $1 \rightarrow r$.

In the case when R is finite consider only those rules $u \rightarrow v$ from S_0 such that $|u| + |v| \leq k + 2$, where $k = \max\{|\ell| + |r| \mid \ell \rightarrow r \in R\}$. Notice, again that all the rules of the type $a \rightarrow ra$ and $a \rightarrow ar$ are in S_0 . \square

Clearly:

$$M(A, \Gamma) = W(A, \Gamma)/S.$$

The following lemma will be used only later. The proof shows however our basic techniques to factorize and to reason about rewriting steps. The reader is therefore invited to read the proof carefully.

Lemma 5.2. *Let $x \in R(A, G)$ be a non-empty G -reduced word. Then $x \xrightarrow[S]{*} y$ implies both $x \xrightarrow[S_0]{*} y$ and y is a non-empty word.*

Proof. By contradiction, assume $x \xrightarrow[S]{*} y$, but not $x \xrightarrow[S_0]{*} y$. Then there are an infinite G -reduced word $u \in R(A, G)$ and some closed word y_0 such that $x \xrightarrow[S_0]{*} y_0 \xrightarrow[S]{*} y$ where the rule $u\bar{u} \rightarrow 1$ applies to y_0 . Note that rules of S_0 replace left-hand sides inside finite intervals. These intervals can be made larger and if two of them are separated by a finite distance, then we can join them. Hence we obtain a picture as follows where all x_i are infinite, and all f_i, g_i are finite words:

$$\begin{aligned} x &= x_1 f_1 \cdots x_{n-1} f_{n-1} x_n \\ y_0 &= x_1 g_1 \cdots x_{n-1} g_{n-1} x_n = p u \bar{u} q, \\ p q &\xrightarrow[S]{*} y, \\ f_i &\xrightarrow[S_0]{*} g_i \text{ for } 1 \leq i \leq n. \end{aligned}$$

The middle position of $y_0 = pu\bar{u}q$ between $u\bar{u}$ cannot be inside some factor x_m as x is G -reduced. The middle position meets therefore some finite factor g_m . Thus, (as u is infinite) we can enlarge f_m such that $f_m \xrightarrow[S_0]{*} 1$. This implies $f_m = g_m = 1$ as words, because x is G -reduced and 1 is irreducible w.r.t. S_0 . Let a be the last letter of u , then it is the last letter of x_m and \bar{a} is the first letter of x_{m+1} , too. Hence $a\bar{a}$ appears as a factor in x . This is a contradiction, and therefore $x \xrightarrow[S_0]{*} y$.

Since x is a non-empty G -reduced word, we cannot have both $x \xrightarrow[S_0]{*} y$ and $y = 1$. \square

The main technical result of this section is the following theorem.

Theorem 5.3. *The system $S \subseteq \Gamma^* \times \Gamma^* \cup R(A, G) \times R(A, G)$ defined in Equation 2 is confluent on $W(A, \Gamma)$.*

For technical reasons we replace the rewrite system $\xrightarrow[S]{*}$ by a new system which is denoted by $\xRightarrow[\text{Big}]{}$. It is defined by

$$\xRightarrow[\text{Big}]{} = \xrightarrow[S_0]{*} \circ \xrightarrow[S]{*} \circ \xrightarrow[S_0]{*}.$$

We have $x \xRightarrow[\text{Big}]{} y$ if and only if there is a derivation $x \xrightarrow[S]{+} y$ which may use many times rules from S_0 , but at most once a rule from the sub system

$$\{u\bar{u} \rightarrow 1 \mid u \in R(A, G) \text{ and } u \text{ is infinite}\}.$$

The notation is due to the fact that we can think of *Big* rules in this subsystem.

The proof of Theorem 5.3 is an easy consequence of the following lemma. However, the proof of this lemma is somehow tedious, technical, and rather long.

Lemma 5.4. *The rewriting system $\xRightarrow[\text{Big}]{}$ is strongly confluent on $W(A, \Gamma)$.*

Proof. We start with the situation

$$y \xleftarrow[\text{Big}]{} x \xrightarrow[\text{Big}]{} z,$$

and we have to show that there is some w with

$$y \xRightarrow[\text{Big}]{\leq 1} w \xleftarrow[\text{Big}]{\leq 1} z.$$

This is clear, if we have $y \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z$, because S_0 is confluent and several steps using $\xRightarrow[\text{Big}]{}$ yield at most one step in $\xRightarrow[\text{Big}]{}$.

Next, we consider the following situation

$$y \xleftarrow[S_0]{*} y_1 \xleftarrow{S} y_0 \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z.$$

We content to find a w such that

$$y_1 \xrightarrow[S_0]{*} w \xleftarrow[\text{Big}]{\leq 1} z.$$

Here comes a crucial observation which is used throughout in the following (compare to the proof of Lemma 5.2). We find factorizations as follows.

$$\begin{aligned} x &= f_0 x_1 f_1 \cdots x_n f_n \\ y_0 &= g_0 x_1 g_1 \cdots x_n g_n \\ z &= h_0 x_1 h_1 \cdots x_n h_n \end{aligned}$$

Moreover, all f_i are finite, all x_i are infinite, and always:

$$g_i \xleftarrow[S_0]{*} f_i \xrightarrow[S_0]{*} h_i.$$

In addition we may assume that $y_0 = pu\bar{u}q$ with $y_1 = pq$ and u is an infinite G -reduced word. We can shrink u by some finite amount and we can make all f_i larger and we can split some x_i into factors. As a consequence we may assume the left-hand side $u\bar{u}$ covers exactly some factor $x_\ell \cdots x_k$ for $1 \leq \ell \leq k \leq n$. In particular, we have

$$y_1 = g_0 x_1 g_1 \cdots x_{\ell-1} g_{\ell-1} g_{k+1} x_{k+1} x_n g_n.$$

Since S_0 is confluent, it is enough to consider the case $x = x_\ell \cdots x_k$. We may therefore simplify the notation and we assume the following:

$$\begin{aligned} x &= x_1 f_1 \cdots x_{n-1} f_{n-1} x_n \\ y_0 &= x_1 g_1 \cdots x_{n-1} g_{n-1} x_n = u\bar{u} \\ z &= x_1 h_1 \cdots x_{n-1} h_{n-1} x_n \\ y_1 &= 1 \end{aligned}$$

We may assume that the middle position between u and \bar{u} is inside some factor g_m . By making f_m larger we may assume that g_m has the form $g_m = r_m \overline{r_m}$. But then we have $h_m \xrightarrow[S_0]{*} 1$, and hence we may assume that $f_m = g_m = h_m = 1$. Refining the partition, making f_i larger, and shrinking u by some finite amount, we arrive at the following situation with $n = 2m$ and

$$y_0 = x_1 g_1 \cdots x_{m-1} g_{m-1} x_m \overline{x_m} \overline{g_{m-1}} \overline{x_{m-1}} \cdots \overline{g_1} \overline{x_1}$$

As $u = x_1 g_1 \cdots x_{m-1} g_{m-1} x_m$ we see that all x_i are G -reduced. For each $1 \leq i \leq m-1$ we find r_i such that $g_i \xrightarrow[S_0]{*} r_i$, $h_i \xrightarrow[S_0]{*} r_i$, and $h_{m+i} \xrightarrow[S_0]{*} \overline{r_{m-i}}$. As a consequence we may assume

$$z = x_1 r_1 \cdots x_{m-1} r_{m-1} x_m \overline{x_m} \overline{r_{m-1}} \overline{x_{m-1}} \cdots \overline{r_1} \overline{x_1}$$

Note that it is not clear that the word $x_1 r_1 \cdots x_{m-1} r_{m-1} x_m$ is G -reduced. So we start looking for a finite non-empty factor h with $h \xrightarrow[S_0]{*} 1$. If we find such a factor, we cancel it and we cancel the corresponding symmetric factor \bar{h} on the right side in $\overline{x_m} \overline{r_{m-1}} \overline{x_{m-1}} \cdots \overline{r_1} \overline{x_1}$. The factor must use a piece of some r_i because all x_i are G -reduced. But it never can use all of some r_i because $x_1 g_1 \cdots x_{m-1} g_{m-1} x_m$ is G -reduced. Thus, the cancellation process stops and we can replace z by some word which has the form $z = v\bar{v}$, where v is indeed G -reduced. Thus, the rewrite step $z \xRightarrow[\text{Big}]{*} 1$ finishes the situation

$$y \xleftarrow[S_0]{*} y_1 \xleftarrow[S]{} y_0 \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z.$$

For later use we recall that we found some w and derivation as follows:

$$y \xrightarrow[S_0]{*} w \xleftarrow[\text{Big}]{\leq 1} z.$$

The challenge is now to consider a situation as follows.

$$y \xleftarrow[S_0]{*} y_1 \xleftarrow[S]{} y_0 \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z_0 \xrightarrow[S]{} z_1 \xrightarrow[S_0]{*} z.$$

We claim that it is enough to find some w with

$$y_1 \xrightarrow[\text{Big}]{\leq 1} w \xleftarrow[\text{Big}]{\leq 1} z_1.$$

Indeed, if such a w exists, then we have just seen that there are w_1, w_2 with

$$y \xrightarrow[\text{Big}]{\leq 1} w_1 \xleftarrow[S_0]{*} w \xrightarrow[S_0]{*} w_2 \xleftarrow[\text{Big}]{\leq 1} z.$$

By confluence of S_0 there is some w' with

$$w_1 \xrightarrow[S_0]{*} w' \xleftarrow[S_0]{*} w_2.$$

We are done, because now

$$y \xrightarrow[\text{Big}]{\leq 1} w' \xleftarrow[\text{Big}]{\leq 1} z.$$

The claim now implies that we are left with the following case:

$$y \xleftarrow[S]{} y_0 \xleftarrow[S_0]^* x \xrightarrow[S_0]^* z_0 \xrightarrow[S]{} z.$$

We repeat the assumptions and notations from above. We have

$$\begin{aligned} x &= f_0 x_1 f_1 \cdots x_n f_n \\ y_0 &= g_0 x_1 g_1 \cdots x_n g_n \\ z_0 &= h_0 x_1 h_1 \cdots x_n h_n \end{aligned}$$

All f_i are finite, all x_i are infinite, and always:

$$g_i \xleftarrow[S_0]^* f_i \xrightarrow[S_0]^* h_i.$$

We may assume that $y_0 = Pu\bar{u}q$ and $z_0 = pv\bar{v}Q$ with $y_1 = Pq$ and $y_1 = pQ$ and u and v are infinite G -reduced words. We can shrink u and v by some finite amount and we can make all f_i larger and we can split some x_i . As a consequence we may assume the left-hand side $u\bar{u}$ covers exactly some factor $x_\ell \cdots x_k$ with $1 \leq \ell \leq k \leq n$, and the left-hand side $v\bar{v}$ covers exactly some factor $x_L \cdots x_K$ with $1 \leq L \leq K \leq n$. We say that g_i is covered by $u\bar{u}$, if $\ell \leq i < k$. If g_i is not covered, then we may assume that $g_i = f_i$. Analogously, h_i is covered by $v\bar{v}$, if $L \leq i < K$. If h_i is not covered, then we may assume that $h_i = f_i$.

We may assume that $\ell \leq L$. If there is no overlap between the factors $u\bar{u}$ and $v\bar{v}$, i.e., if $k < L$, then the situation is trivial, because those g_i or h_i which are not covered, are still equal to f_i . Thus, we have overlap. Moreover, we may assume that $f_0 = f_n = 1$, $\ell = 1$, and $n = \max\{k, K\}$. In order to clarify we repeat

$$\begin{aligned} x &= x_1 f_1 \cdots x_n \\ y_0 &= x_1 g_1 \cdots x_n = u\bar{u}q \\ z_0 &= x_1 h_1 \cdots x_n = pv\bar{v}Q \text{ and either } q = 1 \text{ or } Q = 1 \\ y &= x_{k+1} f_{k+1} \cdots x_{n-1} f_{n-1} x_n \\ z &= x_1 f_1 \cdots x_{L-1} f_{L-1} f_K x_{K+1} \cdots f_{n-1} x_n \end{aligned}$$

We are coming to a subtle point. As above we may assume that the middle position between $u\bar{u}$ is inside some g_m and and that the middle position between $v\bar{v}$ is inside some h_M . There are two cases $m = M$ or $m \neq M$. Let us treat the case $m = M$, first.

Given the preference to u we may enlarge f_m such that $g_m = r\bar{r}$. Thus, actually we may assume $g_m = 1$. However it is not clear that h_m can be factorized the same way. But h_m is finite and v is infinite, hence, by left-right symmetry, we have $h_m = s\bar{s}h$, where $\bar{s}h$ is a prefix of \bar{v} . Now, in the group G we have

$1 = g_m = f_m = h_m = h$. Since h is a factor of \bar{v} and \bar{v} is G -reduced, we conclude that $h = 1$ as a word. This allows to conclude that $f_m = g_m = h_m = 1$ as words. Again, by left-right symmetry, we may assume that \bar{x}_m is a prefix of x_{m+1} . Thus, both in y_0 and in z_0 we replace the common factors $x_m \bar{x}_m$ by 1. Note that this has no influence on y or z . This yields a new assumption about x , y_0 , and z_0 , we have

$$x = x_1 f_1 \cdots x_{n'}$$

with $n' \leq n$ and a corresponding $m' = M' < m$. We repeat the procedure. There is only one way the procedure may stop. Namely at some point v is not an infinite factor anymore.

Hence, we are back at a situation of type:

$$y \xleftarrow[S_0]{*} y_1 \xleftarrow[S]{*} y_0 \xleftarrow[S_0]{*} x \xrightarrow[S_0]{*} z.$$

This situation has already been solved.

Hence for the rest of this proof we may assume $m \neq M$. This is actually the most difficult part. By making f_m and f_M larger, we may assume that $g_m = h_m = 1$ as words. Note that for some letter a we have $x_m = x'a$ and $x_{m+1} = \bar{a}x''$. Assume that h_m is covered by $v\bar{v}$. Then $ah_m\bar{a}$ appears as a non-trivial factor in $v\bar{v}$, where $ah_m\bar{a} \xrightarrow[S_0]{*} 1$. Since both v and \bar{v} are G -reduced, we end up with $m = M$, which has been excluded. Thus, h_m is not covered by $v\bar{v}$. We conclude that we may assume $f_m = g_m = h_m = 1$ as words. By symmetry, g_M is not covered by $u\bar{u}$ and $f_M = g_M = h_M = 1$ as words. In particular we have $k \leq K$. More precisely, we are now faced with the following situation:

$$1 = \ell \leq m \leq L \leq k \leq M \leq K = n.$$

Without restriction we can therefore write:

$$\begin{aligned} x &= x_1 f_1 \cdots x_L f_L \cdots f_{k-1} x_k \cdots f_{n-1} x_n \\ y_0 &= x_1 g_1 \cdots x_{k-1} g_{k-1} x_k f_k x_{k+1} \cdots f_{n-1} x_n = u\bar{u}y \\ z_0 &= x_1 f_1 \cdots x_{L-1} f_{L-1} x_L h_L x_{L+1} \cdots h_{n-1} x_n = zv\bar{v} \\ y &= f_k x_{k+1} \cdots f_{n-1} x_n \\ z &= x_1 f_1 \cdots x_{L-1} f_{L-1} \end{aligned}$$

Consider the *overlapping* factor $\tilde{x} = x_L f_L \cdots f_{k-1} x_k$ inside the word x . Define new words $w_g = x_L g_L \cdots g_{k-1} x_k$ and $w_h = x_L h_L \cdots h_{k-1} x_k$. We claim that

there are G -reduced words U and V such that

$$\begin{aligned} y &\xrightarrow[S_0]{*} V\overline{V}w_h, \\ z &\xrightarrow[S_0]{*} \overline{w}_g U\overline{U}. \end{aligned}$$

By symmetry it is enough to show that $y \xrightarrow[S_0]{*} V\overline{V}w_h$. Consider

$$y_0 = x_1 g_1 \cdots x_{k-1} g_{k-1} x_k f_k x_{k+1} \cdots f_{n-1} x_n.$$

Since $f_M = 1$ we know that $x_L f_L x_{L+1} \cdots f_{M-1} x_M$ reduces to the word v and hence $x_{M+1} f_{M+1} \cdots f_{n-1} x_n$ reduces to \overline{v} . Moreover, we can write $v = w_h V$ with

$$f_k x_{k+1} \cdots f_{M-1} x_M \xrightarrow[S_0]{*} V.$$

As V appears in a factor of v it is G -reduced. We obtain the claim:

$$y = f_k x_{k+1} \cdots f_{M-1} x_M x_{M+1} f_{M+1} \cdots f_{n-1} x_n \xrightarrow[S_0]{*} V\overline{V}w_h.$$

Since S_0 is confluent and $w_g \xleftarrow[S_0]{*} \tilde{x} \xrightarrow[S_0]{*} w_h$, we find w such that

$$\overline{w}_h \xrightarrow[S_0]{*} w \xleftarrow[S_0]{*} \overline{w}_g$$

Hence:

$$y \xrightarrow[\text{Big}]{\leq 1} w \xleftarrow[\text{Big}]{\leq 1} z.$$

This shows that the system S in Equation 2 is confluent. This finishes the proof of the lemma and therefore of Theorem 5.3, too. \square

Corollary 5.5. *The canonical homomorphism $G \rightarrow E(A, G)$ is an embedding.*

Proof. Let $x, y \in \Gamma^*$ be finite words such that $x = y$ in $E(A, G)$. Then we have $x \xrightarrow[S]{*} w \xleftarrow[S]{*} y$ for some $w \in \Gamma^*$. But this implies $x \xrightarrow[S_0]{*} w \xleftarrow[S_0]{*} y$. Hence $x = y$ in G . \square

Corollary 5.6. *Let S_0 be a convergent system defining the group G . The canonical mapping*

$$\text{IRR}(S_0) \cap R(A, G) \rightarrow E(A, G)$$

is injective.

Proof. Since the system S is confluent (hence Church-Rosser), the canonical mapping $\text{IRR}(S) \rightarrow E(A, G)$ is injective. The result follows, because Lemma 5.2 tells us $\text{IRR}(S) \cap R(A, G) = \text{IRR}(S_0) \cap R(A, G)$. \square

The following special case is used in Section 6.

Corollary 5.7. *Let $G = F(\Sigma)$ be a free group. Then pairwise different freely reduced closed words are mapped to pairwise different elements in $E(A, G)$.*

Proof. For $G = F(\Sigma)$ we can choose S_0 to contain just the trivial rules $a\bar{a} \rightarrow 1$, where $a \in \Gamma = \Sigma \cup \Sigma^{-1}$. The system is convergent and

$$\text{IRR}(S_0) = R(A, G) = \{u \in W(A, G) \mid u \text{ is freely reduced}\}.$$

The result follows by Corollary 5.6. \square

Example 5.8. *Let $a \in \Sigma$ and $u, v \in F(\Sigma)$ be represented by non-empty cyclically reduced words in Γ^* . (For example u, v are themselves letters.) Consider the following infinite closed words:*

$$\begin{aligned} w &= [uuu \cdots](\cdots vvv) \\ z &= [uuu \cdots](\cdots aaa)[\bar{a}\bar{a}\bar{a} \cdots](\cdots \bar{v}\bar{v}\bar{v}) \end{aligned}$$

The word w is freely reduced, hence irreducible w.r.t. the system S_0 . The word z is not freely reduced and S_0 is not terminating on z .

By Corollary 5.6 we have $uw = wv$ in $E(A, G)$ if and only if $uw = wv$ in $W(A, G)$ $|u| = |v|$.

Although the word z has no well-defined length one can infer the same conclusion. First let $|u| = |v|$, then $z = uz\bar{v}$ in $E(A, G)$ and hence $uz = zv$. For the other direction write $z = z'\bar{v}$ as words and let $uz = zv = z'$ in $E(A, G)$. Then $uz \xrightarrow[S]{} \tilde{z} \xleftarrow[S]{*} z'$ for some word \tilde{z} .*

After cancellation of factors $a^m\bar{a}^m$ inside $(\cdots aaa) \cdot [\bar{a}\bar{a}\bar{a} \cdots]$ the borderline between a 's and \bar{a} 's must match inside \tilde{z} . So exactly $|u|$ more cancellations of type $a\bar{a} \rightarrow 1$ inside uz took place than in z' . Hence $|u| = |v|$. The other direction is trivial.

For each ordinal $d \in \Omega$ let

$$\mathcal{G}_d = \{x \in E(A, G) \mid x \text{ is given by some word of degree at most } d\}$$

Corollary 5.5 has an obvious generalization. The proof is by transfinite induction and left to the interested reader.

Corollary 5.9. *Let $d \leq e \in \Omega$. Then the canonical homomorphism $\mathcal{G}_d \rightarrow \mathcal{G}_e$ is an embedding.*

The group $E(A, G)$ is the union of all \mathcal{G}_d , but if G is finite nothing interesting happens, we have $G = E(A, G)$ in this case because there are no infinite G -reduced words. However if G is infinite, then $E(A, G)$ may become huge due to the following observation.

Proposition 5.10. *Let A have rank at least 2. Then the following assertions are equivalent:*

i.) *The group G is infinite.*

ii.) *For all $d < e \in \Omega$ we have $\mathcal{G}_d \neq \mathcal{G}_e$.*

Proof. We have $|\Omega| \geq 2$. Let $d < e \in \Omega$ with $\mathcal{G}_d = \mathcal{G}_e$. We show that G is finite. Assume the contrary, then by Lemma 3.1 there is some G -reduced word x of degree e . Assume we find a word z of degree at most d such that $x \xrightarrow[S]{*} z$. Then, by confluence of S we have $x \xrightarrow[S]{*} y \xleftarrow[S]{*} z$ for some y of degree at most d . But now Lemma 5.2 tells us that $x \xrightarrow[S_0]{*} y$, which implies that x is of degree d , too. This is a contradiction, because rules from S_0 cannot decrease any degree other than 0. \square

The notion of a pre-perfect system from Definition 2.4 can be applied to rewriting systems over $W(A, \Gamma)$, too. In this case Theorem 5.3 implies the following result.

Corollary 5.11. *If the group G is defined by some pre-perfect string rewriting system S_0 , then the system S on $W(A, \Gamma)$ is also pre-perfect.*

Definition 5.12. *A word $x \in W(A, \Gamma)$ is called a local geodesic, if it has no finite factor f such that $f = g$ in G and $|g| < |f|$.*

Proposition 5.13. *Let G be presented by some pre-perfect string rewriting system $S_0 \subseteq \Gamma^* \times \Gamma^*$. Let $x \in W(A, \Gamma)$ be a local geodesic. Then $x \xrightarrow[S]{*} y$ implies both $x \xrightarrow[S_0]{*} y$ and $|x| = |y|$.*

Proof. Straightforward from Lemma 5.2 since local geodesics are G -reduced. \square

6 Torsion elements in $E(A, G)$ and cyclic decompositions

This section can be skipped if the reader is interested in the Word Problem of $E(A, G)$, only. We consider an infinite group G and we assume that A is non-Archimedean, i.e., A has rank at least 2. We show that $E(A, G)$ is never torsion

free. More precisely, $E(A, G)$ has always elements of order 2. Actually, often these elements generate $E(A, G)$, see Proposition 6.1. Torsion elements which are not conjugated to torsion elements in G can be represented as infinite fixed points of the involution, i.e., by infinite closed words x satisfying $x = \bar{x}$, see Proposition 6.2. In particular, all "new" torsion elements have order 2.

According to Lemma 3.1 there exists a (non-closed) partial word $p : \mathbb{N} \rightarrow \Gamma$, which is G -reduced. This defines a closed word $[p](\bar{p})$ for each length $(m, 1)$. More formally, for $m \in \mathbb{Z}$ define

$$\begin{aligned} w_m : [(0, 0), (m, 1)] &\rightarrow \Gamma \\ (n, 0) &\mapsto \frac{p(n)}{p(m-n)} \quad \text{for } n \geq 0 \\ (n, 1) &\mapsto \frac{p(m-n)}{p(n)} \quad \text{for } n \leq m \end{aligned}$$

We have $\overline{w_m} = w_m$ and hence $w_m^2 = 1$ in $E(A, G)$. By Theorem 5.3 the element w_m is not trivial, hence w_m has order 2.

In order to make the reasoning more transparent, assume that $G = F(\Sigma)$ is free. Then for $a \in \Sigma$ we may consider closed words $w_m = [aaa \cdots](\cdots \bar{a}\bar{a}\bar{a}) \in W(A, F(\Sigma))$. These words are pairwise different and freely reduced. By Corollary 5.7 reading $w_m \in E((A, F(\Sigma)))$, these elements are still non-trivial, pairwise different, and of order 2.

We have seen that $E(A, G)$ contains infinitely many elements of order 2. Actually, frequently these elements generate $E(A, G)$.

Proposition 6.1. *Let $G = F(\Sigma)$ and $|\Sigma| \geq 2$. Assume that Ω is a limit ordinal, that is for each $d \in \Omega$, we have $d + 1 \in \Omega$, too. Then $E(A, G)$ is generated by elements of order 2.*

Proof. Let x be cyclically reduced with $\deg(x) = d$. (If x is freely reduced, but xx is not, then we can choose some $a \in \Sigma$ such that xa is cyclically reduced since $|\Sigma| \geq 2$.)

We are going to define a freely reduced word x_∞ of length t_{d+1} as follows. For $1 \leq \alpha < t_{d+1}$ we let $x_\infty(\alpha) = x^k(\alpha)$, where $k \in \mathbb{N}$ is large enough that $|x^k| \geq \alpha$. Moreover, we let $x_\infty(t_{d+1} - \alpha + 1) = \overline{x_\infty(\alpha)}$.

Clearly, x_∞ is freely reduced and $\overline{x_\infty} = x_\infty$, hence x_∞ is of order 2. Moreover, by construction, $xx_\infty = x_\infty \bar{x}$. Hence, xx_∞ has order 2, and $x = (xx_\infty)x_\infty$ is the product of two elements of order 2. Since a_∞ is defined for $a \in \Sigma$, we see that all freely reduced words are a product of at most 4 elements of order 2. Now, freely reduced words generate $E(A, F(\Sigma))$, therefore elements of order 2 generate this group. \square

Clearly, as $G \subseteq E(A, G)$, all torsion elements of G appear in $E(A, G)$ again, so we can conjugate them and have many more torsion elements.

Proposition 6.2. *Let $x \in E(A, G)$ be a torsion element which is not conjugated to any element in G . Then there is a reduction $x \xrightarrow[S]{*} y$ such that $y = \bar{y}$. In particular, we have $x^2 = 1 \in E(A, G)$.*

Proof. Choose $x \xrightarrow[S]{*} y$ such that $d \in \Omega$ is minimal and $|y| = n_d t_d + \ell$ with $\deg(\ell) < d$. Moreover, among these y let the leading coefficient $n_d \in \mathbb{N}$ be minimal, too. Note that y cannot contain any factor $uv\bar{u}$ where $\deg(v) < \deg(u) = d$ and $v \xrightarrow[S]{*} 1$. Since x has torsion, we may assume $x^k = 1 \in E(A, G)$ for some $k > 1$. Hence $y^k \xrightarrow[S]{*} 1$ due to confluence of S . Now, $\deg(y^k) = d$, hence $y^k \xrightarrow[S]{*} 1$ implies that y^k has a factor $uv\bar{u}$ where $\deg(v) < \deg(u) = d$ and $v \xrightarrow[S]{*} 1$. Making v larger and u (and \bar{u}) smaller, we can factorize $v = v_1 v_2$ such that uv_1 is a suffix of y and $v_2 \bar{u}$ is a prefix of y . Moreover, for some closed word z of degree d we have $uv_1 \xrightarrow[S]{*} z \xleftarrow[S]{*} u\bar{v}_2$. Hence we can assume that z is a suffix of y and \bar{z} is a prefix of y . If z and \bar{z} overlap in y (that is $|y| < 2|z|$), then we have $y = \bar{y}$. Otherwise we write $y = \bar{z}y'z$ and we replace x by y' and we use induction. \square

7 Group extensions over $A = \mathbb{Z}[t]$

For the remainder of the present paper we assume that $A = \mathbb{Z}[t]$. This means A is the additive group of the polynomial ring over \mathbb{Z} in one variable t . The reason for the choice of A is that we wish the subgroup $A^{\deg < d}$ to be finitely generated for each degree $d \in \Omega$ where:

$$A^{\deg < d} = \{\beta \in A \mid \deg(\beta) < d\}.$$

This assumption is clear for $A = \mathbb{Z}[t]$, because each such subgroup is isomorphic to \mathbb{Z}^d with $d \in \mathbb{N}$. Moreover, every finitely generated subgroup H of $E(A, G)$ sits inside some $E(\mathbb{Z}^d, G)$.

We shall use the following well-known fact:

Lemma 7.1. *Let $k \geq 0$ and*

$$A_0 \subseteq A_1 \subseteq A_2 \subseteq A_3 \cdots$$

be an infinite ascending chain of subgroups in \mathbb{Z}^k . Then this chain becomes stationary, i.e., there is some m such that $A_m = A_n$ for all $n \geq m$.

7.1 Proper periods

Let $w \in W(A, \Gamma)$ be a word of length $\alpha \in A$, given as a mapping $w : [1, \alpha] \rightarrow \Gamma$. An element $\pi \in A$ is called a *period* of w , if for all $\beta \in A$ such that $1 \leq \beta$, $\beta + \pi \leq \alpha$ we have

$$w(\beta) = w(\beta + \pi).$$

A period π is called a *proper period* of w , if $\deg(\pi) < \deg(w)$. In the following we are interested in proper periods, only. We have the following basic lemma.

Lemma 7.2. *Let $w \in W(A, \Gamma)$ of degree $\deg(w) = d$ with $0 \leq d$, then the set $\Pi(w)$ of proper periods forms a subgroup of $A^{\deg < d}$.*

Proof. We have $0 \in \Pi(w)$. If $\pi \in \Pi(w)$, then $-\pi \in \Pi(w)$, too. Let $\pi', \pi \in \Pi(w)$ with $0 \leq \pi' \leq \pi$. Clearly, $\pi + \pi'$ is a proper period, too. It remains to show that $\pi - \pi'$ is a proper period. To see this, let $\beta \in A$ such that $0 \leq \beta$, $\beta + \pi - \pi' \leq |w|$. For $\beta + \pi \leq |w|$ the element $\pi - \pi'$ is a proper period, because then $w(\beta) = w(\beta + \pi) = w(\beta + \pi - \pi')$. Hence we may assume that $\beta + \pi > |w|$. But $\deg(\pi) < \deg(w)$, hence $\deg(\beta) = \deg(w)$ and therefore $0 \leq \beta - \pi'$. Thus, $w(\beta) = w(\beta - \pi') = w(\beta + \pi - \pi')$. \square

Together with Lemma 7.1 the lemma above leads us to the following observation:

Proposition 7.3. *Let $w_0, w_1, w_2, w_3, \dots$ be an infinite sequence of elements of $W(A, \Gamma)$ such that w_{i+1} is always a non-empty factor of w_i . Let*

$$\Pi_0, \Pi_1, \Pi_2, \Pi_3, \dots$$

be the corresponding sequence of proper periods in A . Then this sequence of groups becomes stationary, i.e., there is some m such that $\Pi_m = \Pi_n$ for all $n \geq m$.

Proof. The sequence of degrees is descending and becomes stationary. Hence we may assume that in fact

$$0 \leq \deg(w_0) = \deg(w_1) = \deg(w_2) = \deg(w_3) = \dots$$

As a consequence

$$\Pi_0 \subseteq \Pi_1 \subseteq \Pi_2 \subseteq \Pi_3 \dots$$

is an ascending chain of subgroups in some \mathbb{Z}^k which becomes therefore stationary. \square

8 Deciding the Word Problem in $E(A, G)$

Recall that for a finitely generated group the decidability of the Word Problem does not depend on the presentation: It is a property of the group. In the following we restrict ourselves to the case that Γ is finite (in particular, G is finitely generated). The main difficulty for deciding the Word Problem in $E(A, G)$ is due to periodicity.

8.1 Computing reduced degrees

Let S be the system defined in Equation 2 which is confluent by Theorem 5.3. If we have $x \xrightarrow[S]{*} y$ then we have $\deg(x) \geq \deg(y)$. Thus, we can define the *reduced degree* by

$$\text{red-deg}(x) = \min \left\{ \deg(y) \mid x \xrightarrow[S]{*} y \right\}.$$

Note that $\text{red-deg}(x)$ is well-defined for group elements $x \in E(A, G)$ due the confluence of S .

Lemma 8.1. *Let $u \in R(A, G)$ be a non-empty G -reduced word. Then we have $0 \leq \deg(u) = \text{red-deg}(u)$.*

Proof. This is a direct consequence of Lemma 5.2. □

Clearly, since G is a subgroup of $E(A, G)$, the Word Problem of G must be decidable, otherwise we cannot hope to decide the Word Problem for finitely generated subgroups of $E(A, G)$.

Our goal is to solve the Word Problem in $E(A, G)$ via the following strategy. We compute on input $w \in W(A, \Gamma)$ some $w' \in W(A, \Gamma)$ such that both $w \xrightarrow[S]{*} w'$ and $\deg(w') = \text{red-deg}(w)$. If $\deg(w') > 0$, then $w \neq 1$ in $E(A, G)$. Otherwise w' is a finite word over Γ and we can use the algorithm for G which decides whether or not $w' = 1$ in $G \subseteq E(A, G)$.

In order to achieve this goal we need a slightly stronger condition on G . We need that the non-uniform cyclic membership problem in G is decidable. This means that for each $v \in \Gamma^*$ there is an algorithm $\mathcal{A}(v)$ which solves the problem " $u \in \langle v \rangle$?". Thus, $\mathcal{A}(v)$ decides on input $u \in \Gamma^*$ whether or not u (as an element of G) is in the subgroup of G which is generated by v . This requirement on G is indeed a necessary condition:

Theorem 8.2. *Assume that the Word Problem is decidable for each finitely generated subgroup of $E(A, G)$. Then for each $v \in \Gamma^*$ there exists an algorithm which decides on input $u \in \Gamma^*$ whether or not u (as an element of G) is in the subgroup of G which is generated by v .*

Proof. Let $v \in \Gamma^*$ be a finite word. If v is empty we are done because " $u \in \langle 1 \rangle$?" is nothing but the Word Problem for G (which is a finitely generated subgroup of $E(A, G)$). Hence we may assume that v is non-empty and moreover, $v \neq 1$ in G . If v is a torsion element, then the question whether or not u is in the subgroup generated by v can be reduced to the Word Problem. Hence may assume that $v^k \neq 1$ for all $k \neq 0$. We perform an induction on the length of v which allows to view v as a finite G -reduced word.

We can solve the problem " $u \in \langle v \rangle$?" for all inputs u as soon as we can solve the problem " $u \in \langle pv^k\bar{p} \rangle$?" for some p and $k \neq 0$ for all inputs u . Indeed, fix p and k . Then, $u \in \langle v \rangle$ if and only if $puv^i\bar{p} \in \langle pv^k\bar{p} \rangle$ for some $0 \leq i < |k|$. Clearly, $puv^i\bar{p} \in \langle pv^k\bar{p} \rangle$ implies $u \in \langle v \rangle$. For the other direction let $u = v^m$. We can write $m = \ell k - i$ with $\ell \in \mathbb{Z}$ and $0 \leq i < |k|$. It follows $puv^i\bar{p} \in \langle pv^k\bar{p} \rangle$. Thus, the problem " $u \in \langle v \rangle$?" is reduced to the problem:

$$"\exists i : 0 \leq i < |k| \quad \& \quad puv^i\bar{p} \in \langle pv^k\bar{p} \rangle?"$$

Therefore, by induction on $|v|$ we may assume that no proper factor w of the word v is equal to any $pv^k\bar{p}$ in G . (We only need the existence of an algorithm. There is no need to construct the algorithm on input v .)

Next, we claim that every power v^m is G -reduced. Assume the contrary, then there are words p, q, r, s and $k \in \mathbb{N}$ such that $v = pq = rs$ and $q \neq v \neq r$ as words, but $qv^k r = 1$ in G . Note that neither r nor q can be the empty word by the induction hypothesis. Moreover, $p \neq r$ because $v^{k+1} \neq 1$ in G . If $|p| < |r|$, then we can write $r = pw$ where w is a proper factor of v , and we obtain

$$1 = qv^k pw = \bar{p}pqv^k pw = \bar{p}v^{k+1}pw.$$

This is impossible since no proper factor of v is of the form $pv^{-k-1}\bar{p}$ in G .

If $|p| > |r|$, then $p = rw$ for some proper factor w of v . We obtain $qv^k p = w$ in G . Again this is impossible, because it would imply $qv^k pq\bar{q} = qv^{k+1}\bar{q} = w$ in G .

Thus, $V = [vvv \dots](\dots vvv)$ is a G -reduced word of degree 1 in $E(A, G)$. Next, we may assume that v is a primitive word, this means v is no proper power of any other word. It follows that v does not appear properly inside vv as a factor.

We claim that now, $u \in \langle v \rangle$ if and only if $uV = Vu$ in $E(A, G)$. Clearly, if $u \in \langle v \rangle$ then $uV = Vu$ in $E(A, G)$. For the other direction let $uV = Vu$ in $E(A, G)$. Then by applying finitely many times defining relations for G we must be able to transform the one-sided partial infinite word $uvvv\dots$ into $vvv\dots$. Thus for some word $w \in \Gamma^*$, a factorization $v = pq$, and $k, \ell \in \mathbb{N}$ we obtain $wv^k = v^\ell p$ in G such that the infinite words $wvvv\dots$ and $wqv^k v^{\ell-k} p\dots$ are equal. But v is primitive and hence $p \in \{1, v\}$. Thus, $u \in \langle v \rangle$. \square

Theorem 8.3. *Let G be a group such that for each $v \in \Gamma^*$ there is an algorithm which decides on input $u \in \Gamma^*$ whether or not $u \in G$ is in the subgroup of G generated by v .*

Then for each finite subset $\Delta \subseteq W(A, \Gamma)$ of G -reduced words (i.e., $\Delta \subseteq R(A, G)$) there is an algorithm which computes on input $w \in \Delta^$ its reduced degree and some $w' \in W(A, \Gamma)$ such that both $w \xrightarrow[S]{*} w'$ and $\deg(w') = \text{red-deg}(w)$.*

Proof. The proof is split into two parts. The first part is a preprocessing on the finite set Δ . In the second part we present the algorithm for the set Δ after the preprocessing.

PART I: Preprocessing

The preprocessing concerns Δ and not the actual algorithm. Therefore it is not an issue that the steps in the preprocessing are effective. It is clear that we may replace Δ by any other finite set $\hat{\Delta}$ such that $\Delta \subseteq \hat{\Delta}^*$. This is what we do. We apply the following transformation rules in any order as long as possible, and we stop if no rule changes Δ anymore. The result is $\hat{\Delta}$ which is, as we will see, still a set of G -reduced words. (This will follow from the fact that every factor of a G -reduced word is G -reduced).

- 1.) Replace Δ by $(\Delta \cup \Gamma) \setminus \{1\}$. (Recall that Γ is finite in this section.)
- 2.) If we have $g \in \Delta$, but $\bar{g} \notin \Delta$, then insert \bar{g} to Δ .
- 3.) If we have $g \in \Delta$ with $g = fh$ in $W(A, \Gamma)$ and $\deg(g) = \deg(f) = \deg(h)$, then remove g and \bar{g} from Δ and insert f and h to Δ .

After these steps every element in Δ has its inverse in Δ and for some $d \in \mathbb{N}$ it has a length of the form $t^d + \ell$ with $\deg(\ell) < d$. Thus, the leading coefficient is always 1. In particular, all generators of finite length are letters of $\Gamma = \Sigma \cup \bar{\Sigma}$. The next rules are more involved. We first define an equivalence relation on $W(A, \Gamma)$. We let $g \sim h$ if for some x, y, z, t , and u in $W(A, \Gamma)$ with $\deg(xyzt) < \deg(u)$ we have

$$g = xuy \quad \text{and} \quad h = zut.$$

Note that the condition implies $\deg(g) = \deg(u) = \deg(h)$. The effect of the next rule is that for each equivalence class there is at most one group generator in Δ .

- 4.) If we have $g, h \in \Delta$ with $g \notin \{h, \bar{h}\}$, but $g = xuy$ and $h = zut$ for some x, y, z, t , and u with $\deg(xyzt) < \deg(u)$, then remove g, h, \bar{g}, \bar{h} from Δ and insert x, y, z, t (those which are non-empty) and u to Δ .

- 5.) If we have $g \in \Delta$ with $g \neq \bar{g}$, but $g = xuy = z\bar{u}t$ for some x, y, z, t , and u with $\deg(xyzt) < \deg(u)$, then write $u = pq$ with $\deg(p) < \deg(q) = \deg(u)$ and $q = \bar{q}$. Remove g and \bar{g} from Δ and insert x, y, z, t, p, \bar{p} (those which are non-empty) and q to Δ . (Note that $g \sim q$.)

The next rules deal with periods.

- 6.) If we have $g \in \Delta$ and $g = xuy$ for some x, y , and u with $\deg(xy) < \deg(u)$ such that u has a proper period which is not a period of g , then remove g, \bar{g} from Δ and insert x, y (those which are non-empty) and u to Δ .

The following final rule below makes Δ larger again, and the rule adds additional information to each generator. For each $g \in \Delta$ let $\Pi(g) \subseteq A$ the group of proper periods. Let $B(g)$ be a set of generators of $\Pi(g)$. We may assume that for each possible degree d there is at most one element $\beta \in B(g)$ of degree d . Moreover, we may assume $0 \leq \beta$ and for each g the set $B(g)$ is fixed. In particular, for $\pi \in \Pi(g)$ with $\deg(\pi) = d \geq 0$ there is exactly one $\beta \in B(g)$ such that $\deg(\beta) = d$ and $\pi = m\beta + \ell$ for some unique $m \in \mathbb{Z}$ and $\ell \in \Pi(g)$ with $\deg(\ell) < d$. For each $\beta \in B(g)$ let $r(\beta)$ be the prefix and $s(\beta)$ be the suffix of length β of g . (In particular, $r(\beta)g = gs(\beta)$ in $W(A, \Gamma)$.) Note that the number of $r(\beta), s(\beta)$ is bounded by $2 \deg(g)$.

- 7.) If we have $g \in \Delta$, then let $B(g)$ be a set of generators for the set of proper periods $\Pi(g)$ as above. If necessary, enlarge Δ by finitely many elements of degree less than $\deg(g)$ (and which are factors of elements of Δ) such that $r(\beta), s(\beta) \in \Delta^*$ for all $\beta \in B(g)$.

Note that the rules 1.) to 7.) can be applied only a finite number of times. The formal proof relies on König's Lemma and Proposition 7.3.

Remark 8.4. *Note that the preprocessing has been done in such a way that every element in $\hat{\Delta}$ is either a letter or a factor of an element in the original set Δ . In particular, if Δ contains local geodesics only, then $\hat{\Delta}$ has the same property. This fact is used for Corollary 8.6.*

PART II: An algorithm to compute the reduced degree

We may assume that Δ has passed the preprocessing, i.e., $\Delta = \hat{\Delta}$ and no rule above changes Δ anymore. The input w (to the algorithm we are looking for) is given as a word $g_1 \cdots g_n$ with $g_i \in \Delta$. Let

$$d = \max \{ \deg(g_i) \mid 1 \leq i \leq n \}.$$

We may assume that $d > 0$. Either $\deg(w) = \text{red-deg}(w)$ (and we are done) or $\deg(w) > \text{red-deg}(w)$ and $w \in W(A, \Gamma)$ contains a factor $uv\bar{u}$ such that the following conditions hold:

- 1.) The word u is G -reduced and has length $|u| = t^d + \ell$ with $\deg(\ell) < d$,
- 2.) $\deg(v) < d$,
- 3.) $v \xrightarrow[S]{*} 1$.

We may assume that the factor $uv\bar{u}$ starts in some g_i and ends in some g_j with $i < j$, because the leading coefficient of each length $|g_i| \in \mathbb{Z}[t]$ is 1. Moreover, by making u smaller and thereby v larger, we may in fact assume that u is a factor of g_i and \bar{u} is a factor of g_j . Thus, $\deg(g_i) = \deg(u) = \deg(g_j) = d$ and we can write $g_i = xuy$ and $g_j = z\bar{u}t$. By preprocessing on Δ (Rule 4), we must have $g_i \in \{g_j, \bar{g}_j\}$. Assume $g_i = g_j$, then we have $g_i = xuy = z\bar{u}t$ and, by preprocessing on Δ (Rule 5), we may conclude $g_i = \bar{g}_i$. Thus in any case we know $g_i = \bar{g}_j$.

Thus, henceforth we can assume that for some $1 \leq i < j \leq n$ we have in addition to the above:

- 4.) $g_i = xuy$,
- 5.) $v = yg_{i+1} \cdots g_{j-1}z$,
- 6.) $g_j = z\bar{u}t = \bar{g}_i$.

Since $g_j = z\bar{u}t = \bar{g}_i$ we have $xuy = \bar{t}u\bar{z}$, and by symmetry (in i and j) we may assume:

- 7.) $|y| \geq |z|$.

This implies $y = q\bar{z}$ for some $q \in W(A, \Gamma)$ with $\deg(q) < d$ and $uq = q'u$ for $\bar{t} = xq'$.

Therefore $|q|$ is a proper period of u , and hence, by preprocessing on Δ (Rule 6), we see that $|q|$ is a proper period of g_i . Thus there are $p', p \in \Delta^*$ with $|p'| = |p| = |q|$ such that $p'g_i = g_ip$. But \bar{z} and y are suffixes of g_i , hence

$$y = \bar{z}p.$$

Therefore:

- 8.) $pg_{i+1} \cdots g_{j-1} \xrightarrow[S]{*} 1$, where p is a suffix of g_i and $|p|$ is a proper period of g_i .

We know $\deg(g_{i+1} \cdots g_{j-1}) < d$. Hence by induction on d we can compute $h \in \Delta^*$ such that both $g_{i+1} \cdots g_{j-1} \xleftarrow[S]{*} h$ and $\deg(h) = \text{red-deg}(g_{i+1} \cdots g_{j-1})$. This implies $\deg(h) = \text{red-deg}(p)$, too. But p is a factor of a G -reduced word, hence actually $\deg(h) = \deg(p)$ by Lemma 8.1.

We distinguish two cases. Assume first that $\deg(h) \leq 0$. Then $h, p \in \Gamma^*$ are finite words. If $h = 1$ in G , then we can replace the input word w by

$$g_1 \cdots g_{i-1} g_{j+1} \cdots g_n$$

since $g_i g_{i+1} \cdots g_{j-1} \bar{g}_i \xrightarrow[S]{*} 1$, and we are done by induction on n .

If $h \in \Gamma^*$ is a finite word, but $h \neq 1$ in G , then $p = h^{-1} \neq 1$ in G , too. Consider the smallest element $\rho \in B(g_i)$ and let $r \in \Gamma^*$ be the suffix of g_i with $|r| = \rho$. It follows that p is a positive power of r because $|p|$ is a period of g_i . This means that h is in the subgroup of G generated by r . For this test we have an algorithm by our hypothesis on G . According to our assumptions the answer of the algorithm is yes: h is in the subgroup generated by r . This allows to find $m \in \mathbb{Z}$ with $\bar{h} = r^m$ in the group G . We find some finite word s of length $|s| = |r^m|$ such that $sg_i = g_i r^m$; and we can replace the input word w by $g_1 \cdots g_{i-1} \bar{s} g_{j+1} \cdots g_n$, because we have:

$$\begin{aligned} g_1 \cdots g_i \cdots g_j \cdots g_n &\xleftrightarrow[S]{*} g_1 \cdots \bar{s} s g_i \cdots g_j \cdots g_n \\ &\xleftrightarrow[S]{*} g_1 \cdots \bar{s} g_i r^m h \bar{g}_i g_{j+1} \cdots g_n \\ &\xrightarrow[S]{*} g_1 \cdots \bar{s} g_i \bar{g}_i g_{j+1} \cdots g_n \\ &\xrightarrow[S]{} g_1 \cdots g_{i-1} \bar{s} g_{j+1} \cdots g_n. \end{aligned}$$

We are done by induction on the number of generators of degree d .

The final case is $\deg(h) > 0$. We write $|h| = m't^e + \ell$ with $\deg(\ell) < e = \deg(h)$. According to our preprocessing on Δ (Rule 7) there are words $r, s \in \Delta^*$ such that $\deg(r) = \deg(p)$, r is a suffix of g_i with $sg_i = g_i r$. For some m with $m \leq m'$ we must have $\text{red-deg}(r^m h) < e$. By induction we can compute some word f with $\deg(f) = \text{red-deg}(r^m h)$ and $f \xleftrightarrow[S]{*} r^m h$. Like above we can replace the input word w by

$$g_1 \cdots g_{i-1} \bar{s}^m g_i f g_j \cdots g_n,$$

because we have:

$$\begin{aligned} g_1 \cdots \bar{s}^m s^m g_i \cdots g_j \cdots g_n &\xleftrightarrow[S]{*} g_1 \cdots \bar{s}^m g_i r^m h \bar{g}_i g_{j+1} \cdots g_n \\ &\xleftrightarrow[S]{*} g_1 \cdots \bar{s}^m g_i f \bar{g}_i g_{j+1} \cdots g_n. \end{aligned}$$

We are done by induction on the degree e which is the reduced degree of the factor $r^m g_{i+1} \cdots g_{j-1}$. We can apply this induction since $g_i r^m g_{i+1} \cdots g_{j-1} g_j$ now has a factor $uv\bar{u}$ such that the following conditions hold:

- 1.) The word u is G -reduced and $\deg(u) = d > 0$,

$$2.) \deg(v) < e,$$

$$3.) v \xrightarrow[S]{*} 1.$$

□

By Theorems 8.2 and 8.3 we obtain the following corollary which gives the precise answer in terms of the group G whether or not the Word Problem in finitely generated subgroups of $E(A, G)$ is decidable.

Corollary 8.5. *Let G be finitely generated by Γ and $A = \mathbb{Z}[t]$. Then the following assertions are equivalent:*

- i.) *For each $v \in \Gamma^*$ there is an algorithm which decides on input $u \in \Gamma^*$ the Cyclic Membership Problem " $u \in \langle v \rangle$?"*
- ii.) *For each finite subset $\Delta \subseteq W(A, \Gamma)$ there is an algorithm which decides on input $w \in \Delta^*$ whether or not $w = 1$ in the group $E(A, G)$.*

Recall that (according to Definition 5.12) a local geodesic denotes word without any finite factor f such that $f = g$ in G but $|g| < |f|$. Inspecting the proof above we find the following variant of Corollary 8.5.

Corollary 8.6. *Let G be finitely generated by Γ and $A = \mathbb{Z}[t]$. Then the following assertions are equivalent:*

- i.) *The group G has a decidable Word Problem.*
- ii.) *For each finite subset $\Delta \subseteq W(A, \Gamma)$ of local geodesics there is an algorithm which decides on input $w \in \Delta^*$ whether or not $w = 1$ in the group $E(A, G)$.*

Remark 8.7. *Clearly, Condition i.) in Corollary 8.5 implies Condition i.) in Corollary 8.6, but the converse fails. There is a finitely presented group G with a decidable Word Problem, but one can construct a specific word v such that the Cyclic Membership Problem " $u \in \langle v \rangle$?" is undecidable, see [24, 25].*

Remark 8.8. *Let G be a finitely generated group. Of course, if G has a decidable Generalized Word Problem, i.e., the Membership Problem w.r.t. finitely generated subgroups is decidable, then the Cyclic Membership Problem " $u \in \langle v \rangle$?" is decidable, too. Examples of groups G where the Generalized Word Problem is decidable include metabelian, nilpotent or, more general, abelian by nilpotent groups, see [27]. However, there are also large classes of groups, where the Membership Problem is undecidable, but the Cyclic Membership Problem is easy. For example, the Cyclic Membership Problem is decidable in linear time in a direct*

product of free groups, but as soon as G contains a direct product of free groups of rank 2, the Generalized Word Problem becomes undecidable by [20]. For hyperbolic groups a construction of Rips shows that the Generalized Word Problem is undecidable ([26]), but the Cyclic Membership Problem " $u \in \langle v \rangle$?" is decidable by [19].

Decidability of the the Cyclic Membership Problem is also preserved e.g. by effective HNN extensions. This means, if H is an HNN-extension of G by a stable letter t such that we can effectively compute Britton reduced forms, then one can reduce the Cyclic Membership Problem " $u \in \langle v \rangle$?" in H to the same problem in G as follows. On input u, v we compute first the Britton reduced form of v . This tells us whether $v \in G$. If so, we are done by checking first that $u \in G$ and then by using the algorithm for G . So, let $v \in H \setminus G$. Via conjugation we may assume that v^k remains Britton reduced for all $k \in \mathbb{Z}$. Now, if u is Britton reduced, too, then it is enough to check $u = v^k$ for that k where the t -sequence of u coincides with the one of v^k . There is at most one such k . Thus we can use the algorithm to decide the Word Problem in H which exists because we can effectively compute Britton reduced forms.

As every one-relator group G sits inside an effective HNN extension of another one-relator group with a shorter relator [18], we see that the Cyclic Membership Problem is decidable in one-relator groups, too. The property is also preserved by effective amalgamated products for a similar reason as for HNN extensions.

9 Realization of some HNN-extensions

The purpose of this section is to show that the group $E(A, G)$ contains some important HNN-extensions of G which therefore can be studied within the framework of infinite words. Moreover, we show that $E(A, G)$ realizes more HNN-extensions than it is possible in the approach of [22]. The reason is that [22] is working with cyclically reduced decompositions, only. We begin with this concept and we show first how it embeds in our setting.

9.1 Cyclically decompositions for freely reduced words

In [22] a partial multiplication on freely reduced words and a partial monoid $\text{CDR}(A, \Sigma)$ has been defined for a free group $F(\Sigma)$: Let $x, y \in R(A, F(\Sigma))$ be freely reduced words. The partial multiplication $x * y$ is defined if and only if $x = pq$, $y = \bar{q}r$, and pr is freely reduced. In this case $x * y = pr$.

As a set $\text{CDR}(A, \Sigma)$ consists of those freely reduced words x , which admit a *cyclically reduced decomposition* $x = cu\bar{c}$ where u is cyclically reduced. If the decomposition exists, it is unique. Note that $c = [aaa \cdots](\cdots \bar{a}\bar{a}\bar{a})$ is freely

reduced, but it is not in $\text{CDR}(A, \Sigma)$. On the other hand, for $a \neq b \in \Sigma$ we have

$$x = [aaa \cdots)(\cdots \bar{a}\bar{a}\bar{a}baaa \cdots)(\cdots \bar{a}\bar{a}\bar{a}] \in \text{CDR}(A, \Sigma)$$

since $x = cb\bar{c}$.

In terms of the group $E(A, F(\Sigma))$ we can rephrase this as follows. The set $\text{CDR}(A, \Sigma)$ embeds into $E(A, F(\Sigma))$ because all elements are freely reduced and hence irreducible by the confluent system S . Now, $\text{CDR}(A, \Sigma)$ (being a subset of a group) becomes a partial monoid by restricting the definition of $x * y$ to the case where $x * y = xy$ is defined and $xy \in \text{CDR}(A, \Sigma)$. If $xy \notin \text{CDR}(A, \Sigma)$, then the result $x * y$ remains undefined.

Now, assume x, y , and $xy \in \text{CDR}(A, \Sigma)$. Then there exists a freely reduced word $z = cw\bar{c}$ where w is cyclically reduced such that $xy \xrightarrow[S]{*} z$. The reduction provides us with a factorization such that $x = pq$, $y = \bar{q}r$, and pr is freely reduced. Thus, $x * y$ is defined. In this way the partial monoid $\text{CDR}(A, \Sigma)$ embeds naturally into the group $E(A, F(\Sigma))$.

Let $a, b \in \Sigma$ with $a \neq b$. It is known that the HNN-extension of $F(\Sigma)$ by $sbs^{-1} = a$ with stable letter s embeds into $\text{CDR}(A, \Sigma)$ with $s = [aaa \cdots)(\cdots bbb]$. To see this, observe that this HNN-extension can be written as a semi-direct product $F(a, b) \rtimes \mathbb{Z}$. This allows to write elements in normal form as a word $x = w \cdot s^k$ where w is a freely reduced word over Σ^\pm and $k \in \mathbb{Z}$. A direct inspection shows that x is in $\text{CDR}(A, \Sigma)$ and it is trivial in $E(A, F(\Sigma))$ if and only if it is trivial in $F(a, b) \rtimes \mathbb{Z}$.

However, the HNN-extension H of G by $sb^2s^{-1} = a^2$ does not embed into $\text{CDR}(A, \Sigma)$ because the commutation relation \sim is not transitive, but it is known to be transitive in any finitely generated subgroup of $\text{CDR}(A, \Sigma)$, [2]. The commutation relation is not transitive in H , because $a \sim a^2 = sb^2s^{-1} \sim sbs^{-1}$, but $a \not\sim sbs^{-1}$ in H .

The group $E(A, F(\Sigma))$ is however large enough to realize the HNN extension H , but we have to leave $\text{CDR}(A, \Sigma)$: Define

$$s = [aaa \cdots)(\cdots ababab \cdots)(\cdots bbb].$$

Then the canonical homomorphism $H \rightarrow E(A, F(\Sigma))$ is an embedding. (See Proposition 9.4.) Note that $sb^2s^{-1} = a^2$, but $sbs^{-1} \neq a$ due to the middle line of ab 's which requires a shift by 2 in order to be matched. Clearly, $s, b, \bar{s} \in \text{CDR}(A, \Sigma)$ and $s' = s * b \in \text{CDR}(A, \Sigma)$ is defined. But $s' * \bar{s}$ is not defined, and therefore $sbs^{-1} \in E(A, F(\Sigma)) \setminus \text{CDR}(A, \Sigma)$. (Note that $s \cdot b \cdot s^{-1}$ is not a cyclically reduced decomposition, because $sb\bar{s}$ is not freely reduced and there is no freely reduced word x such that $x = sbs^{-1} \in E(A, F(\Sigma))$.) The element $s'\bar{s} = sb\bar{s}$ can be depicted as follows:

$$sb\bar{s} = [aaa \cdots)(\cdots ababab \cdots)(\cdots bbb][\bar{b}\bar{b} \cdots)(\cdots bababa \cdots)(\cdots bb]b.$$

Remark 9.1. Let H be a subgroup inside the partial monoid $\text{CDR}(A, \Sigma)$, then H is torsion-free. Indeed $(cu\bar{c})^2 = cu^2\bar{c}$ and we can use Proposition 6.2. Since sbs^{-1} is torsion-free and $sbs^{-1} \in E(A, F(\Sigma)) \setminus \text{CDR}(A, \Sigma)$ for s and b as above, we see that the set of torsion elements is a proper subset of $E(A, F(\Sigma)) \setminus \text{CDR}(A, \Sigma)$, in general.

We conclude this subsection with a few more examples which allow similar calculations as above. In these examples we use however stable letters which have no cyclically reduced decomposition.

Example 9.2. Consider the following non-abelian semi-direct products: $G_1 = \mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})$ (which is isomorphic to the free product $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$) and $G_2 = \mathbb{Z} \rtimes \mathbb{Z}$. (which is isomorphic to the Baumslag-Solitar group $\text{BS}(1, -1)$.) The groups G_1 and G_2 can be embedded into $E(\mathbb{Z} \times \mathbb{Z}, \mathbb{Z})$. Indeed, define s_1 and s_2 as follows:

$$\begin{aligned} s_1 &= [aaa \cdots)(\cdots \bar{a}\bar{a}\bar{a}], \\ s_2 &= [aaa \cdots)(\cdots aaaa \cdots)(\cdots \bar{a}\bar{a}\bar{a}]. \end{aligned}$$

The element s_1 has order 2 and s_2 has infinite order in $E(\mathbb{Z} \times \mathbb{Z}, \mathbb{Z})$. Clearly $as_i = s_i\bar{a}$, and it is easy to verify that the subgroups generated by a and s_i are isomorphic to G_i for $i = 1, 2$.

Let $\Sigma \geq 2$ and let G_3 be the HNN-extension of \mathbb{Z} with stable letter s and defining relation $s^{-1}a^2s = a^{-2}$. The group G_3 is also the Baumslag-Solitar group $\text{BS}(2, -2)$. It embeds into $E(\mathbb{Z} \times \mathbb{Z}, F(\Sigma))$ using s_3 as a stable letter, where

$$s_3 = [aaa \cdots)(\cdots ababab \cdots)(\cdots \bar{a}\bar{a}\bar{a}].$$

Again, a direct verification that this group embeds is not difficult. All three embeddings occur as special cases of Proposition 9.4. None of these groups can be embedded into the partial monoid $\text{CDR}(A, \Sigma)$: The group G_1 is not torsion free and the commutation relation is not transitive neither in G_2 nor in G_3 .

9.2 Some HNN-extensions in $E(A, G)$

We continue with the assumption that $A = \mathbb{Z}[t]$. In [22] a power x^t with length $|x| \cdot t$ is constructed for $x \in \text{CDR}(A, \Sigma)$. (The partial monoid $\text{CDR}(A, \Sigma)$ has been defined in Section 9.1.) The construction of x^t fails however to satisfy $\bar{x}^t = \overline{x^t}$, in general. Thus, x^t cannot be used to define an HNN extension with stable letter x^t . We content ourselves to prove the following fact.

Proposition 9.3. *Let $x \in W(A, G)$ be a non-empty cyclically G -reduced word. Then we can define a free abelian subgroup X of $E(A, G)$ with countable basis $\{x_d \mid d \in \mathbb{N}\}$ such that $x_0 = x$. Hence, the homomorphism*

$$a_0 + a_1 t + \cdots + a_n t^n \mapsto x^{a_0} (x_1)^{a_1} \cdots (x_n)^{a_n}$$

embeds the abelian group A into $E(A, G)$.

Proof. Let $\deg(x) = e \geq 0$ and $|x| = \alpha$.

For $k \in \mathbb{N}$ consider x^{2k} as a mapping $x^{2k} : [-k\alpha + 1, k\alpha] \rightarrow \Gamma$. We can extend this to a partial (non-closed) word $x^{\mathbb{Z}} : D \rightarrow \Gamma$, where the domain is $D = \{\delta \in \mathbb{Z}[t] \mid \deg(\delta) \leq e\}$. Note that $\bar{x}^{\mathbb{Z}}(\delta) = x^{\mathbb{Z}}(-\delta + 1)^{-1}$ for $\delta \in D$.

We define $x_A : A \rightarrow \Gamma$ as follows: We let $x_A(\beta) = x^{\mathbb{Z}}(\beta)$ for $\deg(\beta) \leq e$. For $\deg(\beta) > e$ write $\beta = t^{e+1}\gamma + \delta$ with $\delta \in D$; and let $x_A(\beta) = x^{\mathbb{Z}}(\delta)$.

Finally, let $x_0 = x$ and for every $d \geq 1$ let x_d be the restriction of x_A to the closed interval $[1, t^{e+d}]$.

The word x_d has length t^{e+d} and $|x|$ is a proper period. We have to show that $\bar{x}_d = (\bar{x})_d$ for $d \geq 1$. To see this, consider $1 \leq \beta \leq t^{e+d}$ and write $\beta = t^{e+1}\gamma + \delta$ with $\delta \in D$. Then:

$$\begin{aligned} \bar{x}_d(\beta) &= x_d(t^{e+d} - t^{e+1}\gamma - \delta + 1)^{-1} \\ &= x^{\mathbb{Z}}(-\delta + 1)^{-1} \\ &= \bar{x}^{\mathbb{Z}}(\delta) \\ &= (\bar{x})_d(\beta) \end{aligned}$$

Thus, $a_0 + a_1 t + \cdots + a_n t^n \mapsto x^{a_0} (x_1)^{a_1} \cdots (x_n)^{a_n}$ is a homomorphism of abelian groups.

Assume $f(t) = a_0 + a_1 t + \cdots + a_n t^n \mapsto 1 \in E(A, G)$, then $a_n = 0$ due to the degrees and the fact that x is a cyclically G -reduced word. By induction $f(t) = 0$. \square

We say that a non-empty word $w \in W(A, G)$ is *primitive* if first w does not appear as a factor of ww other than as its prefix or as its end and second \bar{w} is not a factor of ww . In particular, a primitive word does not have any non-trivial proper period. If on the other hand, we can write $ww = pwq$ with $1 \leq |p| < |w|$, then $|p|$ is a non-trivial period of w . Note that the word w which looks like $[ababab \cdots](\cdots ababab)$ has period 2, it is not primitive, but it is no power of any other element. Hence, unlike to the case of finite words, being primitive is a stronger condition than not being a power of any other element.¹

¹A power is an element u^k for $k \in \mathbb{Z}$ since we have not defined u^α for $\deg(\alpha) > 0$. However even in a more general context the assertions remain true: assume w and w' look like $[ababab \cdots](\cdots ababab)$ with $w = (ab)^\alpha$ and $w' = (ab)^\beta$, where $|w| = t$ and $|w'| = t + 1$. Then we should expect that $(ab)^{\beta-\alpha}$ is a power of ab , but this is not compatible with $|(ab)^{\beta-\alpha}| = 1$.

Note also that $ww = p\bar{w}q$ means that we can write $w = pq$ with $\bar{p} = p$ and $\bar{q} = q$. It follows that w is primitive if and only if \bar{w} is primitive. For a non-abelian free group $F(\Sigma)$ primitive cyclically reduced words of every positive length exist: Consider w with $w(1) = a$ and $w(\beta) = b$ otherwise.

Let H be a subgroup of $E(A, G)$ and $u \in H$ be a cyclically G -reduced element. As usual the *centralizer* of u in H is the subgroup $\{v \in H \mid uv = vu\}$.

Proposition 9.4. *Let H be a finitely generated subgroup of $E(A, G)$ and let $u, v, w \in H$ be (not necessarily different) cyclically G -reduced elements such that $|u| = |v| = |w|$ and such that w is primitive. In addition, let u and v have cyclic centralizers in H . Then the HNN extension*

$$H' = \langle H, t \mid s^{-1}us = v \rangle$$

embeds into $E(A, G)$.

Proof. Let $\deg(u) = e$. We have $e \geq 0$. Since H is finitely generated, there is a degree d (with $d > e$) such that $\deg(x) < d$ for all $x \in H$. By the construction according to Proposition 9.3 we define the following elements $U = u_{d-e-1}$, $V = v_{d-e-1}$, and $W = w_{d-e-1} \in E(A, G)$. Recall that $|U| = |V| = |W| = |w|$ for $d = e + 1$ or $|U| = |V| = |W| = t^{d-1}$ for $d > e + 1$. The abelian group of proper periods $\Pi(W)$ is trivial or it is generated by $|w|$ and t^{e+1}, \dots, t^{d-2} . The groups $\Pi(U)$ and $\Pi(V)$ may have larger rank than $d - e$.

Let us define a word s of length $2t^d$ which is depicted as follows:

$$s = [UUU \dots](\dots WW \dots)(\dots VVV).$$

The group $\Pi(s)$ is generated by $|w|$ and t^{e+1}, \dots, t^{d-1} . As u is a prefix of U , v is a suffix of V , and $|u| = |v| = |w|$ is a proper period of s , we see that $us = sv$. Thus, we obtain a canonical homomorphism $\varphi : H' \rightarrow E(A, G)$. We have to show that φ is injective. For this it is enough to consider a Britton-reduced word in H' which begins with s or with \bar{s} . We can write this word as a sequence $s^{\varepsilon_1}y_1 \dots s^{\varepsilon_n}y_n$ with $\varepsilon_i = \pm 1$ and $y_i \in H$ for $1 \leq i \leq n$ and we may assume that $n \geq 1$.

If the word is trivial in $E(A, G)$, then it must contain a factor of the form $\bar{x}zx$ where $\deg(z) < \deg(x) = \deg(s)$, $|x|$ has leading coefficient 1, and $z = 1 \in E(A, G)$. Moreover, (by symmetry and by making x shorter if necessary) we may assume that x or \bar{x} can be depicted as $[UUU \dots](\dots WWW)$. No such factor $\bar{x}zx$ appears inside s or \bar{s} . Thus, we have $n \geq 2$ and we may assume that $\bar{x}zx$ is a factor of $s^{\varepsilon_1}y_1s^{\varepsilon_2}$. Assume that $\varepsilon_1 = \varepsilon_2$, say $\varepsilon_1 = \varepsilon_2 = 1$, then $\bar{x}zx$ appears inside

$$[UUU \dots](\dots WW \dots)(\dots VVV)y_1[UUU \dots](\dots WW \dots)(\dots VVV).$$

It is also clear that the factor z must match some factor inside the middle part $(\dots VVV)y_1[UUU \dots]$. But the word w is primitive, hence \bar{w} is no factor of ww and w is a factor of $\bar{w}\bar{w}$. Therefore this is actually impossible.

Note that the arguments remain valid even if e.g. $u = \bar{v}$ (which is the least evident case). Then $U = \bar{V}$ and infinitely many cancellations inside s^2 are possible, but nevertheless inside

$$[\bar{V}\bar{V}\bar{V}\dots)(\dots WW\dots)(\dots VVV][\bar{V}\bar{V}\bar{V}\dots)(\dots WW\dots)(\dots VVV]$$

there is no factor $\bar{x}zx$ with degree $\deg(s) = \deg(x) > \deg(z)$.

The conclusion is $\varepsilon_1 = -\varepsilon_2$ and we may assume $\varepsilon_1 = -1$. We therefore may assume that $\bar{x}zx$ is a factor inside the word $\bar{s}ys$ with $y = y_1 \in H$. Making z longer and x shorter we may assume that y is a factor of the word z , and z has the form $\bar{U}_1 y U_2$ where U_1, U_2 are prefixes of $[UUU\dots]$. Without restriction we have $U_1 = U^n$ and $|U_1| \leq |U_2|$. Since \bar{x} appears as a suffix of \bar{s} we may indeed assume that x has the form $[UUU\dots)(\dots WWW]$. The word x begins (inside the word s) with $puu\dots$, where $|p| < |u|$. More precisely, $|U_2|$ is a proper period of x , and we can write $|U_2| = \beta t^{e+1} + m|u| - |p|$ for some $\beta \in \mathbb{Z}[t]$, $m \in \mathbb{Z}$, and suffix p of u . By Lemma 7.2 $|p|$ is a proper period of x and in turn $|p|$ is a period of the word ww . Since w is primitive we conclude $p = 1$, thus $|U_2| = \beta t^{e+1} + m|u|$. In particular, U_2 ends with $(\dots uu]$ and we see that actually $U_1 = U^n$ is a suffix of U_2 . Replacing x by $U^n x$ we may assume that the factor z has the form yU' . We conclude that U' is a prefix of $[UUU\dots]$ and $U' \in H$ (because $y \in H$ and $z = 1 \in E(A, G)$).

It is now enough to show that $U' \in \langle u \rangle$. Write $|U'| \equiv \alpha \pmod{t^{e+1}}$ with $\deg(\alpha) \leq e$. Note that $|U'| = |U_2| - n|U|$ is still a proper period of x . Thus, as above we see that $\alpha = k|u|$ for some $k \in \mathbb{Z}$. This implies that U' is in the centralizer of u and U' is cyclically G -reduced. In particular, $\deg U'^m = \text{red-deg}(U'^m)$ for all $m \in \mathbb{Z}$. By hypothesis the centralizer of u is cyclic, hence for some element $r \in E(A, G)$ and some $\ell, m \in \mathbb{Z}$ we obtain $U' = r^\ell$, $u = r^m$. It follows $U'^m = u^\ell \in E(A, G)$. Hence $\deg U' \leq e = \deg(u)$, too. We conclude

$$|U'| = \alpha = k|u|.$$

As U' is a prefix of $[UUU\dots]$, we see that $U' = u^k$; and the result is shown. \square

References

- [1] R. Alperin and H. Bass. Length functions of group actions on Λ -trees. *Combinatorial group theory and topology*, 111:265–378, 1987.
- [2] H. Bass. Group actions on non-Archimedean trees. In *Arboreal group theory (Berkeley, CA, 1988)*, volume 19 of *Math. Sci. Res. Inst. Publ.*, pages 69–131. Springer, New York, 1991.

- [3] M. Bestvina and M. Feighn. Stable actions of groups on real trees. *Invent. Math.*, 121(2):287–321, 1995.
- [4] R. Book and F. Otto. *Confluent String Rewriting*. Springer-Verlag, 1993.
- [5] I. Chiswell. *Introduction to Λ -trees*. World Scientific, 2001.
- [6] I. Chiswell and T. Muller. Embedding theorems for tree-free groups. Under consideration.
- [7] V. Diekert, A. J. Duncan, and A. G. Myasnikov. Geodesic rewriting systems and pregroups. In O. Bogopolski, I. Bumagin, O. Kharlampovich, and E. Ventura, editors, *Combinatorial and Geometric Group Theory*, Trends in Mathematics, pages 55–91. Birkhäuser, 2010.
- [8] A. M. G. Baumslag and V. Remeslennikov. Residually hyperbolic groups. *Proc. Inst. Appl. Math. Russian Acad. Sci.*, 24:3–37, 1995.
- [9] D. Gaboriau, G. Levitt, and F. Paulin. Pseudogroups of isometries of \mathbb{R} and Rips’ theorem on free actions on \mathbb{R} -trees. *Israel. J. Math.*, 87:403–428, 1994.
- [10] M. Jantzen. *Confluent String Rewriting*, volume 14 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, 1988.
- [11] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. I: Irreducibility of quadratic equations and Nullstellensatz. *J. of Algebra*, 200:472–516, 1998.
- [12] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. II: Systems in triangular quasi-quadratic form and description of residually free groups. *J. of Algebra*, 200(2):517–570, 1998.
- [13] O. Kharlampovich and A. Myasnikov. Implicit function theorems over free groups. *J. of Algebra*, 290:1–203, 2005.
- [14] O. Kharlampovich and A. Myasnikov. Elementary theory of free non-abelian groups. *J. of Algebra*, 302:451–552, 2006.
- [15] O. Kharlampovich, A. Myasnikov, V. Remeslennikov, and D. Serbin. Groups with free regular length functions in \mathbb{Z}^n . To appear, arXiv:0907.2356v2.
- [16] O. Kharlampovich, A. Myasnikov, V. Remeslennikov, and D. Serbin. Subgroups of fully residually free groups: algorithmic problems. In A. G. Myasnikov and V. Shpilrain, editors, *Group theory, Statistics and Cryptography*, volume 360, pages 63–101, 2004.

- [17] R. Lyndon. Groups with parametric exponents. *Trans. Amer. Math. Soc.*, 9:518—533, 1960.
- [18] R. Lyndon and P. Schupp. *Combinatorial Group Theory*. Classics in Mathematics. Springer, 2001.
- [19] I. Lysenok. On some algorithmic problems of hyperbolic groups. *Math. USSR Izvestiya*, 35:145–163, 1990.
- [20] K. A. Mihailova. The occurrence problem for direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958. English translation in: *Math. USSR Sbornik*, 70: 241–251, 1966.
- [21] J. Morgan and P. Shalen. Valuations, trees, and degenerations of hyperbolic structures. *I. Annals of Math*, 120(3):401–476, 1984.
- [22] A. Myasnikov, V. Remeslennikov, and D. Serbin. Regular free length functions on Lyndon’s free $\mathbb{Z}[t]$ -group $F^{\mathbb{Z}[t]}$. *Contemp. Math., Amer. Math. Soc.*, 378:37–77, 2005.
- [23] A. Nikolaev. *Membership Problem in Groups Acting Freely on Non-Archimedean Trees*. Doctor of philosophy, McGill University, Montreal, Quebec, August 2010.
- [24] A. Y. Olshanskii and M. V. Sapir. Length functions on subgroups in finitely presented groups. In *Groups — Korea’98 (Pusan)*. de Gruyter, 2000.
- [25] A. Y. Olshanskii and M. V. Sapir. Length and area functions on groups and quasi-isometric Higman embeddings. *IJAC*, 11(2):137–170, 2001.
- [26] E. Rips. Subgroups of small cancellation groups. *Bull. London Math. Soc.*, 14:45–47, 1982.
- [27] N. S. Romanovskii. The occurrence problem for extensions of abelian by nilpotent groups. *Sib. Math. J.*, 21:170–174, 1980.
- [28] J.-P. Serre. *Trees*. New York, Springer, 1980.
- [29] J. Stallings. *Group theory and three-dimensional manifolds*. Yale University Press, New Haven, Conn., 1971. A James K. Whittemore Lecture in Mathematics given at Yale University, 1969, Yale Mathematical Monographs, 4.

Volker Diekert, Universität Stuttgart, Universitätsstr. 38, 70569 Stuttgart, Germany
 Alexei Myasnikov, Stevens Institute of Technology, Hoboken, NJ 07030, USA